TESTIMONY OF

PARRY AFTAB, ESQ.

**(THE KIDS INTERNET LAWYER and
FOUNDER and EXECUTIVE DIRECTOR, WIREDSAFETY.ORG, THE WORLD'S LARGEST AND OLDEST INTERNET SAFETY and HELP ORGANIZATION)**

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON COMMERCE, SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

**JULY 11, 2006, 10:00 A.M.
RAYBURN HOUSE OFFICE BUILDING, ROOM 2123**

***Social Networks and 109th Congress 2d Session H.R. 5319
The "Deleting Online Predators Act of 2006"***

Parry Aftab, Esq.
Executive Director, WiredSafety.org
Email:parry@aftab.com
www.aftab.com
201-463-8663

TABLE OF CONTENTS

SUMMARY ***3***

OPENING STATEMENT ***6***

Exhibit A: Overview of WiredSafety.org ***14***

Exhibit B: Parry Aftab's Bio and CV: ***18***

APPENDIXES: ***24***

Appendix 1: ***25***

Appendix 2: ***29***

Appendix 3: ***30***

Appendix 4: ***33***

Appendix 5: How schools are handling these issues ***35***

Appendix 6: ***39***

Appendix 7: ***41***

Appendix 8: ***43***

Appendix 9: Parenting Online ***54***

SUMMARY

Our children are online. They do their homework, entertain themselves, communicate with each other and us, research things, shop for things and compare prices online. They need the Internet for their education, their careers and for their future. Of all the risks our children face online, only one is certain. If we deny our children access to these technologies, we have guaranteed that they are hurt. All other risks are avoidable through a combination of awareness, supervision, parental control and other technologies and the adoption of best practices by schools and the Internet industry itself. More and more children being lured and stalked by online predators who gather information about them from social networking profiles, chatrooms, instant messaging, e-mails and websites and who use this information and access to "groom" them.

With our children walking around with Internet access in their backpacks and pocketbooks, we can no longer rely on parents watching whatever they do from a central location computer. Our children need to learn to use the "filter between their ears" and "ThinkB4TheyClick." This requires that we get them involved in framing solutions and educating each other. It also requires that we find new ways of building good cyber-citizenship and helping the kids and parents spot risks in new technologies and protect themselves online. It also requires that we engage the Internet industry itself in ways to build safer technologies and adopt best practices designed to make all their users, not just children, safer.

Social networking, a combination of mini-web pages, blogs and searchable communities, have expanded in recent years, most recently exploding with the growth of MySpace.com. Parry Aftab estimates that more than half of the young teens in the US with home Internet access have at least one social networking profile. Some were set up by their friends, and others by the young teens themselves. Many have 2 to 5 separate profiles on just one site, and most have at least one profile on two or more social networks (not all being used, however). WiredSafety.org first began its social networking safety work in 2004, after learning how many young teens and preteens were beginning to use them. Unlike the early AOL profile pages used by teens and preteens in prior years, where the young users could post their contact information and brief statements about their interests, these networks were designed to be interactive. And instead of dry posts of contact and other personal interest information, these networks allowed teens to use html coding to add music, movies, animations, sounds, images and lots of user generated content to their page.

While the media and many others have focused only on the dangers of these networks when used by preteens and teens, it is important that we also explore their good uses and value and why their use has exploded in the last year and a-half. We have spent two years studying how and why preteens and teens use these kinds of sites.

Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. And sadly, in some cases, our teens are acting out, taking risks and seeking romance online (even knowingly with adults). That's when things can get dangerous, especially for young teens.

Our preteens and teens are often intentionally sharing risky information online in profiles, blogs and on websites. They may also share this information with stranger unwittingly, such as posting their cell numbers on their public away messages when using IM technologies. They intentionally post graphically sexual images and engage in and post cybersexual communications on their profiles and in chat-type technologies. And even when they are careful about protecting their own privacy, they may not be safe from their friends - even well-meaning friends. Their close friends may expose personal information about them by posting photos and information on their profiles.

They are also, in greater and greater numbers, meeting people offline that they met online. In 2000, Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. I believe that these numbers, when revised, will disclose that many more are doing this than 5 years ago. It is becoming more commonplace. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

Smart kids are sharing sexual images online with people they don't know, or e-mailing them to others they have a crush on and hope to entice. And with the newer video-chats, webcams and similar technologies, the predators have moved to luring our kids into posing and engaging in sexually explicit activities entirely online, in the comfort of their bedrooms, with parents sitting unwittingly downstairs.

And while we focus on sexual predators online and how they are using social networks and community interactive technologies to reach our children, we too often forget that the most prevalent risk our children face on these networks and using these technologies is cyberbullying, not adult sexual predators. A vast majority of the preteen and young teens we polled have been involved, directly or indirectly, in at least one cyberbullying incident. They torment and terrorize each other. They threaten and embarrass each other. They post fake profiles, hateful messages and steal each other's passwords and identities, all designed to bully their victims. They do it in groups, singly, openly and anonymously. They use cell phones, interactive gaming devices and sites and web profiles, blogs and websites where you can vote for the ugliest, fattest, least popular or gayest student. And schools are the ones most impacted, when students who might be creating and posting these hateful communications from home or otherwise outside of school ground and after-hours, become engaged in violence and hurtful interactivities during school hours. In addition, when our teens and preteens are posting real or fantasy information about how much alcohol they consumed at this weekend's party, or how active their sex life has become, or how they cheated on their finals or shoplifted from the local mall, they may not realize that college recruiters, scholarship committees, coaches and future employers can access this information in years to come. This is an increasingly growing risk our children pose to themselves.

All of this has schools concerned. Private schools, especially, are facing real challenge controlling their students' activities online. Facebook.com is favored by private and parochial school students, who are impressed with the fact that it was formed at Harvard

and other private and parochial students can be found there. It has, as some teens tell us, the "snob factor."

Our children are sometimes accessing these sites from their school laptops, in-classroom desktops and school and public libraries. So, a parent's "house rules" may not have much effect when their child leaves the house. So, creating a new law prohibiting schools and libraries from allowing underage students and users to access these sites is an obvious approach. But is the answer to these problems found in laws restricting where students can go during school hours on school computers? Or can this be controlled by blocking access to interactive community networking sites, such as MySpace, Facebook and others from public and school libraries? While this may appear on its face to be an easy answer, it is neither easy nor the answer.

As more social networks are launched every day, and every ISP, entertainment company and wireless provider is either building a social network or finding a way to integrate social networking and community interactivity into their new and existing sites, it is impossible to block all of them and not other valuable Internet features, sites and content. Instead, schools need to be armed with the tools and risk management expertise to decide what sites their students can access during school hours from their servers and how to enforce their decisions and policies.

Schools need to decide if their students should have access to *any* non-educational site from school computers, and if so, which ones and for what purpose. They then need to develop a policy communicating this decision and the rules to the students (in language they understand), the teachers, the parents and other caregivers and to their IT team. They need to decide whether they will be using software to help enforce their policy, or merely traditional discipline for violating school policies. That too needs to be communicated to the school community. They also need to create or adopt educational programs teaching their students what information they can and shouldn't be sharing online, the risks of irresponsible Internet use and where to go when things go wrong. They can play an important role in teaching parents and other community members about safe, private and responsible Internet and wireless technologies use.

Educators, not legislators, should be deciding what students do during the school day. They know their students and the learning environment best. But schools do need the guidance and help of legislators and regulators to do this right. They need reliable information and studies on which they can base their decisions. They need to be apprised of new trends and developing risks. They need to know that websites and services are using the latest and best technologies and have adopted the best industry practices with their users' safety in mind. They need help that Congress can provide.

Congress can also be very helpful in helping gather relevant information about cybercrimes and abuses. I have testified previously that actual cybercrime statistics are lacking. Everything we know is largely anecdotal. In 1999, the FBI's Innocent Images (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my estimates, about the same number of cases were opened by state and local law enforcement agencies that year. The same year, approximately 25 million minors used the Internet in the U.S. Now, with more than 75 million young Internet users in the U.S. we don't know if the number of instances have increased, decreased or remain flat, given the growth. The crime reporting forms don't collect information about

the use of the Internet is child sexual exploitation crimes, or any other crimes. That has to change.

Creating a central reporting database where all instances of cybercrimes are reported for statistical purposes, from cyberharassment to Internet-related ID theft, fraud and scams, to sexual predators and Internet-related child pornography and sexual exploitation would be incredibly helpful. It could track cybercrime trends affecting adults, seniors and youth. It could be used to help design safer systems and best practices and guide legislation directed at a meaningful problem, in a meaningful way.

In addition, with tax dollars becoming more and more precious and the mission of all Congressional representatives to put tax dollars into the most effective use, existing programs by trusted non-profit groups can be highlighted and made available online to schools and community organizations that need them, without cost. Without having to reinvent the wheel, massive amounts of programs, lesson plans and risks management guides already exist that can be used as is, or easily retooled. Finding a way to get these wonderful resources into the hands of those who need them the most, using interactive technologies and the Internet and mobilizing volunteers to help deploy existing programs that were developed with or without government dollars is the fastest way to make a dent in the problem. Focusing attention on what works and what doesn't is something that Congress does best. WiredSafety.org and I pledge our help in doing that.

It's time.

OPENING STATEMENT

SOCIAL NETWORKS AND COMMUNITY INTERACTIVE TECHNOLOGIES AND US TEENS AND PRETEENS

WiredSafety has been involved in cybersafety for ten years (see the attached description of our organization and work in the Appendix). It was founded and is run by Parry Aftab, one of the first Internet lawyers specializing in security and privacy law. She is frequently referred to as "The Kids Internet Lawyer" for her work with the children's online industry and child privacy issues and is an unpaid volunteer. For ten years we have cautioned Internet users of all ages against sharing too much personal information online, through profiles (pre-social networking), websites and online and mobile chat technologies. So we could quickly adapt our expertise to the new social networking explosion. It is crucial that this Sub-Committee recognizes that social networking is the future of the Internet and cyber-communications. It is here to stay and being used by every major ISP and cyber-industry, by every trusted brand online and offline. It is not limited to newcomers, such as MySpace and Facebook, but includes Google, AOL, Microsoft, Yahoo! and others. Coming to terms with how and why people are using these networks is essential.

There are always trends in what kids are doing online. And some, that may have started as a trend, become core technologies adopted by adults and businesses alike. Instant-messaging and social networks head this list. Social networks (sometimes incorrectly called "blogs") are the future of the Internet and cyber-technology. They are a cross between an online diary, a cyberdating network, an online publishing house, the fastest way to reach out to your friends online and a place to share your creativity and express yourself – on steroids.

MySpace grew in popularity because it offered what teens wanted - the ability to express themselves in any way they could imagine if they could locate or write the code to do it. But, interestingly enough, when MySpace was created, it was designed for independent musicians age 18 - 34, not for teens and preteens. It was the teens who found MySpace, not the other way around. By February 2005, when I first called them with our concerns, MySpace had approximately 6 million users/profiles. By late May, 2005, they had approximately 23 million users/profiles. By the end of 2005 that had increased to approximately 50 million users/profiles and stands at about 90 million users/profiles today. Until recently, our safety tips appeared on MySpace as their safety page, and we were the only watchdog within the site. We remain the only watchdog within most of the other major social networks, but no longer populate MySpace's safety pages or take abuse reports from their users. This is now handled internally by MySpace.

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. It also allows them to network with others online. Sometimes people do this to find romance. Sometimes they do it to find friends with similar interests. While this may be okay for adults, it is not okay for kids and may not be okay for young teens without parental supervision.

Most social-networking websites agree and prohibit anyone under a certain age from using their website. Unfortunately, while they may set rules to keep younger teens and preteens off the site, they can't prevent kids from lying about their age and pretending to be old enough to use the website. (These sites are typically free and, without a payment or age verification or authentication, they never know who their members are in real life.) To address the lying some sites have developed special software applications designed to help identify underage members by reviewing the contents of member profiles. It's not perfect, but it does help spot many underage members.

I recently visited a Marine Base in Yuma, Arizona and worked with teens and preteens on the base. I polled many of the preteens, learning that several of them had a "MySpace." When I pointed out MySpace's minimum age requirement of 14, they shrugged and explained that they were "mature for their age." After a 45-minute presentation, these same preteens knew far more about protecting themselves on MySpace and similar sites. But they still wanted to keep their "MySpace" profiles. This is a problem parents, schools, library media specialists and others are facing. How do you keep preteens and teens off of the social networks? Parents are told to talk with their kids,

While no one can always tell if someone is lying about their age, some of these sites use some method of age verification or authentication (such as Facebook.com's college e-mail address requirement for their college users or YFly.com's field team approach). And these and others really try to keep underage users off their site. Many other similar sites do not. So, when allowing any teen to use a social-networking website, even with supervision, it helps to make sure it's a trustworthy one. WiredSafety allows those we consider more trustworthy to use our safety tips and link to our help teams. So, looking for our tips is a good way to start finding the sites we consider more trustworthy. In addition, our new seal program that will review sites for compliance with best practices, privacy and safety practices will launch in September.[1] This should help in telling the good and

[1] The seal will deal with several issues impacting safety, such as their law enforcement policies (how easy it is for law enforcement agencies to work with the site when cybercrimes and abuses are reported or in conducting

responsible players from the bad and irresponsible ones.

All ISPs, entertainment companies and major wireless providers either already have a social network or similar community feature or will over the next year. New ones are launched daily. I am contacted by leading venture capitalists and investor groups daily to advise on a new proposal or network. The top five or six networks with substantial US user-bases claim, collectively, almost 200 million user profiles. Even if one user may set up several profiles (I have learned that most 12-16 year olds have between 2 and 5 different profiles, each set up with a different e-mail address), it is estimated that at least 80 million people are using social networks in the US.[2] I have polled approximately 10,000 teens and preteens face-to-face across the US over the last four months on their social network usage. These sites include MySpace.com, Xanga.com, Bebo.com, Tagged.com, BlackPlanet.com and its sister site, MiGente.com, and FaceBook.com, among others.

We have learned a great deal about why kids use these kinds of sites. Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes. They stage protests from their profiles new millennium-style, letting policymakers know how they feel about the propose immigration policies and other issues important to teens, in interactive petitions. They make and share news. They engage in educational activities, such as building profiles of their favorite historical characters. One user may write music and another he has never met may write the lyrics. It's where they hang out and have fun, share their expertise and talents and find others like themselves. Or, they may be looking for other teens with lives radically different from theirs - farm-kids may want to find city-kids or conservative kids may want to find outrageous ones. They can try on different guises and lifestyles and pretend to be

---

investigations, how long they maintain IP data to assist in tracking the identity of cybercriminals and the location of missing children, and how well they inform law enforcement about what information they collect and retain and how to legally request it), safety (privacy and security settings, abuse reporting mechanisms, the expertise of their abuse reporting staff, their terms of service and how well they are enforced), their customer service (how they handle request from parents and schools, how easy it is to remove or modify a profile, how well they educate their users about safety and security, their technological protections against malicious code and ID theft, and their relationship with high-risk sites) and if they cater to preteens or teens, how carefully they care for their interests (such as how well they comply with the child-protection privacy rules and laws and how sensitive they are to appropriate marketing and advertising practices and placement and how well they handle cyberbullying and other youth-centric abuses).

[2] Some websites, including MySpace.com, make it very difficult to remove a profile. In MySpace's case, the user must fill out an online form to request instructions on profile deletion and a special code will be e-mailed to the non-MySpace e-mail they used when setting up their account for them to use to shut down their profile page. Due to the fact that many users either use a fake e-mail address to protect their privacy or have since stopped using the one they provided when the account was set-up, the code cannot be delivered. Even if the e-mail address is real and still functioning, however, many ISPs and e-mail providers block MySpace communications sent over their networks as SPAM. Without the code, the profiles remain up, even if the user wants them removed, which may lead to inflated user-numbers. (WiredSafety has arranged for a special process to assist in the removal of teen/preteen profiles when the e-mail address is not working, but I suspect that it is not widely used unless the user comes to us for our assistance.)

someone they aren't, both good and bad.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. But most of our teens aren't there for meeting strangers or checking out provocative photos. Sadly, in some cases, though, they are acting out, taking risks and seeking romance online. That's when things can get dangerous, for users of all ages, but especially young teens. (You can learn more about Internet sexual predators and how they operate at our new site for preventing and helping young victims of Internet sexual predators, Katiesplace.org.)

Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes. They stage protests from their profiles new millennium-style, letting policymakers know how they feel about the propose immigration policies and other issues important to teens, in interactive petitions. They make and share news. They engage in educational activities, such as building profiles of their favorite historical characters. One user may write music and another he has never met may write the lyrics. It's where they hang out and have fun, share their expertise and talents and find others like themselves. Or, they may be looking for other teens with lives radically different from theirs - farm-kids may want to find city-kids or conservative kids may want to find outrageous ones. They can try on different guises and lifestyles and pretend to be someone they aren't, both good and bad.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. And sadly, in some cases, our teens are acting out, taking risks and seeking romance online (even knowingly with adults). That's when things can get dangerous, especially for young teens.

Our preteens and teens are often intentionally sharing risky information online in profiles, blogs and on websites. They may also share this information with stranger unwittingly, such as posting their cell numbers on their public away messages when using IM technologies. They intentionally post graphically sexual images and engage in and post cybersexual communications on their profiles and in chat-type technologies. And even when they are careful about protecting their own privacy, they may not be safe from their friends - even well-meaning friends. Their close friends may expose personal information about them by posting photos and information on their profiles.

They are also, in greater and greater numbers, meeting people offline that they met online. In 2000, Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. I believe that these numbers, when revised, will disclose that many more are doing this than 5 years ago. It is becoming more commonplace. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

Smart kids are sharing sexual images online with people they don't know, or e-mailing them to others they have a crush on and hope to entice. And with the newer video-chats, webcams and similar technologies, the predators have moved to luring our kids into

posing and engaging in sexually explicit activities entirely online, in the comfort of their bedrooms, with parents sitting unwittingly downstairs.

And while we focus on sexual predators online and how they are using social networks and community interactive technologies to reach our children, we too often forget that the most prevalent risk our children face on these networks and using these technologies is cyberbullying, not adult sexual predators. A vast majority of the preteen and young teens we polled have been involved, directly or indirectly, in at least one cyberbullying incident. They torment and terrorize each other. They threaten and embarrass each other. They post fake profiles, hateful messages and steal each other's passwords and identities, all designed to bully their victims. They do it in groups, singly, openly and anonymously. They use cell phones, interactive gaming devices and sites and web profiles, blogs and websites where you can vote for the ugliest, fattest, least popular or gayest student. And schools are the ones most impacted, when students who might be creating and posting these hateful communications from home or otherwise outside of school ground and after-hours, become engaged in violence and hurtful interactivities during school hours. In addition, when our teens and preteens are posting real or fantasy information about how much alcohol they consumed at this weekend's party, or how active their sex life has become, or how they cheated on their finals or shoplifted from the local mall, they may not realize that college recruiters, scholarship committees, coaches and future employers can access this information in years to come. This is an increasingly growing risk our children pose to themselves.

Our preteens and teens are often intentionally sharing risky information online in profiles, blogs and on websites. They may also share this information with stranger unwittingly, such as posting their cell numbers on their public away messages when using IM technologies. They intentionally post graphically sexual images and engage in and post cybersexual communications on their profiles and in chat-type technologies. And even when they are careful about protecting their own privacy, they may not be safe from their friends - even well-meaning friends. Their close friends may expose personal information about them by posting photos and information on their profiles.

They are also, in greater and greater numbers, meeting people offline that they met online. In 2000, Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. I believe that these numbers, when revised, will disclose that many more are doing this than 5 years ago. It is becoming more commonplace. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

Smart kids are sharing sexual images online with people they don't know, or e-mailing them to others they have a crush on and hope to entice. And with the newer video-chats, webcams and similar technologies, the predators have moved to luring our kids into posing and engaging in sexually explicit activities entirely online, in the comfort of their bedrooms, with parents sitting unwittingly downstairs.

And while we focus on sexual predators online and how they are using social networks and community interactive technologies to reach our children, we too often forget that the most prevalent risk our children face on these networks and using these technologies is cyberbullying, not adult sexual predators. A vast majority of the preteen and young teens we polled have been involved, directly or indirectly, in at least one cyberbullying incident.

They torment and terrorize each other. They threaten and embarrass each other. They post fake profiles, hateful messages and steal each other's passwords and identities, all designed to bully their victims. They do it in groups, singly, openly and anonymously. They use cell phones, interactive gaming devices and sites and web profiles, blogs and websites where you can vote for the ugliest, fattest, least popular or gayest student. And schools are the ones most impacted, when students who might be creating and posting these hateful communications from home or otherwise outside of school ground and after-hours, become engaged in violence and hurtful interactivities during school hours. In addition, when our teens and preteens are posting real or fantasy information about how much alcohol they consumed at this weekend's party, or how active their sex life has become, or how they cheated on their finals or shoplifted from the local mall, they may not realize that college recruiters, scholarship committees, coaches and future employers can access this information in years to come. This is an increasingly growing risk our children pose to themselves.

All of this has schools concerned. Private schools, especially, are facing real challenge controlling their students' activities online. Facebook.com is favored by private and parochial school students, who are impressed with the fact that it was formed at Harvard and other private and parochial students can be found there. It has, as some teens tell us, the "snob factor." Teens need to be on a social network to have a social life these days. (Although many are leaving MySpace in favor of other sites, for various reasons.)

But there's more to it. When I polled an average of 5000 kids every month on this, I learned that they love the creativity of it. They love expressing themselves so others can appreciate it. They enjoy adding sparkly graphics and sharing their stories, poems and jokes. One of the Teenangels (WiredSafety's expert teen and preteen program, teenangels.org) told me that it's all about "Pink! Pink! Pink!" She can build a page using pink font, on a black background and feel creative and cool. (Her mother is an interior decorator and she has to wear a school uniform, and saw this as her sole expressive outlet.)

As important as allowing them to express themselves in a creative way is, though, it's not enough to get me to do a turn-about with these kinds of sites and teens. I was very negative about these sites. I have now taken a second look after talking to another one of my Teenangels.

This Teenangel (a soft-spoken and gentle girl) did a research project on social networking websites. She reviewed some of these sites and listed the kinds of risks young teens face on these websites. She then went on to explain that she had several profiles online at these sites. I was initially shocked and disappointed that one of my expert teens would take such risks with their personal information when they knew better. When I asked her why she would do such a risky thing, as the Teenangels often do, this one taught me something new.

She explained that it's hard being a young teen these days. Few kids in the school will give you the chance to see how much you have to offer unless you are the captain of the cheerleading squad or of the debate team. A profile page that is open to the other students at your school gives you a chance to share the special things about yourself with them, and will help them get to know you better. It's about sharing your favorite movies and books, about sharing fun vacation memories and your dreams, it's about sharing how special you are. It's about helping you make friends in your school with people who

appreciate you. It's not about strangers, it's about others in their class.

There is a real value to that. Whether it's by posting a profile page that is supervised by their parents, or building a website. It can be pink and sparkly, or thoughtful and inspiring. But it's all about who your teen is or who they want to be. It's a challenge to give them a place where they can express themselves while keeping them safe, protected from predators and from sharing too much private information online. But if you are willing to supervise what they are saying and doing on their profiles, I'm willing to help.

Lying on their pages is part of what this is all about, too. They pretend to be older (and not just to get around the age restrictions), richer, more famous or more popular. Boys pretend to be girls and girls pretend to be boys. They may be tall blonde surfers from Malibu or live on a ranch in New Zealand. While this may not be a problem, some of their other kinds of pretending can be dangerous for teens in a public social network.

They may act tougher than they are in real life "rl," provoke other, or talk about getting drunk, or their sexuality. They may pose as someone they don't like, to cyberbully and harass them, or steal their identities. I have spent years protecting children from predatorial adults. I never thought I would be spending as much time as I am protecting them from each other. But, they are using these sites by the millions. And their use will only grow. So, I advise the thousands of parents who e-mail us daily and those who review our safety tips online that on how to handle the issue and that they need to be the parent.[3]

Our children are sometimes accessing these sites from their school laptops, in-classroom desktops and school and public libraries. So, a parent's "house rules" may not have much effect when their child leaves the house. So, creating a new law prohibiting schools and libraries from allowing underage students and users to access these sites is an obvious approach. But is the answer to these problems found in laws restricting where students can go during school hours on school computers? Or can this be controlled by blocking access to interactive community networking sites, such as MySpace, Facebook and others from public and school libraries? While this may appear on its face to be an easy answer, it is neither easy nor the answer.

As more social networks are launched every day, and every ISP, entertainment company and wireless provider is either building a social network or finding a way to integrate social networking and community interactivity into their new and existing sites, it is impossible to block all of them and not other valuable Internet features, sites and content. Instead, schools need to be armed with the tools and risk management expertise to decide what sites their students can access during school hours from their servers and how to enforce their decisions and policies.

Schools need to decide if their students should have access to *any* non-educational site from school computers, and if so, which ones and for what purpose. They then need to develop a policy communicating this decision and the rules to the students (in language they understand), the teachers, the parents and other caregivers and to their IT team. They need to decide whether they will be using software to help enforce their policy, or merely traditional discipline for violating school policies. That too needs to be communicated to the school community. They also need to create or adopt educational

[3] See attached advice for parents, in Appendix.

programs teaching their students what information they can and shouldn't be sharing online, the risks of irresponsible Internet use and where to go when things go wrong. They can play an important role in teaching parents and other community members about safe, private and responsible Internet and wireless technologies use.

Educators, not legislators, should be deciding what students do during the school day. They know their students and the learning environment best. But schools do need the guidance and help of legislators and regulators to do this right. They need reliable information and studies on which they can base their decisions. They need to be apprised of new trends and developing risks. They need to know that websites and services are using the latest and best technologies and have adopted the best industry practices with their users' safety in mind. They need help that Congress can provide.

Congress can also be very helpful in helping gather relevant information about cybercrimes and abuses. I have testified previously that actual cybercrime statistics are lacking. Everything we know is largely anecdotal. In 1999, the FBI's Innocent Images (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my estimates, about the same number of cases were opened by state and local law enforcement agencies that year. The same year, approximately 25 million minors used the Internet in the U.S. Now, with more than 75 million young Internet users in the U.S. we don't know if the number of instances have increased, decreased or remain flat, given the growth. The crime reporting forms don't collect information about the use of the Internet is child sexual exploitation crimes, or any other crimes. That has to change.

Creating a central reporting database where all instances of cybercrimes are reported for statistical purposes, from cyberharassment to Internet-related ID theft, fraud and scams, to sexual predators and Internet-related child pornography and sexual exploitation would be incredibly helpful. It could track cybercrime trends affecting adults, seniors and youth. It could be used to help design safer systems and best practices and guide legislation directed at a meaningful problem, in a meaningful way.

In addition, with tax dollars becoming more and more precious and the mission of all Congressional representatives to put tax dollars into the most effective use, existing programs by trusted non-profit groups can be highlighted and made available online to schools and community organizations that need them, without cost. Without having to reinvent the wheel, massive amounts of programs, lesson plans and risks management guides already exist that can be used as is, or easily retooled. Finding a way to get these wonderful resources into the hands of those who need them the most, using interactive technologies and the Internet and mobilizing volunteers to help deploy existing programs that were developed with or without government dollars is the fastest way to make a dent in the problem. Focusing attention on what works and what doesn't is something that Congress does best. WiredSafety.org and I pledge our help in doing that.

It's time.

Exhibit A: Overview of WiredSafety.org

WiredSafety.org is a 501(c) (3) charity and the largest and oldest online safety, education, and help group in the world. It consists of thousands of volunteers from more than 76 countries around the world, all working online with the mission of promoting a safer and more responsible Internet and wireless experience for everyone.

Originating in 1995 as a group of volunteers rating websites, it now provides one-to-one help, extensive information, and education to cyberspace users of all ages and members of the Internet industry on a myriad of Internet and interactive technology safety issues. These services are offered through a worldwide organization comprised entirely of volunteers who administer specialized websites and programs. WiredSafety.org volunteers range in age from 18 to 80 and run the gamut from TV personalities, teachers, law enforcement officers, PhD's, writers and librarians to stay-at-home moms, retired persons, and students. WiredSafety.org's founder and Executive Director, cyberlawyer Parry Aftab, is also an unpaid volunteer. With the exception of its TeenAngels, outreach and speaking programs, all work and help is provided online and free of charge.

WiredSafety.org's work falls into four major areas, all designed to help promote a safer and more responsible digital experience for everyone:

- **Assistance** for victims of cyberabuse and harassment and others who need help online, including parents, teens and educators.

- **Advice, Training and Help** for law enforcement worldwide on preventing, spotting and investigating cybercrimes and for members of the Internet and interactive digital industries in designing safer technologies and adopting and implementing best practices.

- **Education** for children, parents, communities, law enforcement, abuse and customer help staff within the Internet industry and professional development for educators.

- **Information and Awareness** on all aspects of online safety, privacy, responsible use and security wired, wireless and as new technologies are developed.

Our target audiences include:

- Parents, grandparents and caregivers (including aunts, uncles and older siblings);
- Pre-reader lap-surfers, kids, preteens, teens and college students;
- Members of the Internet, wireless and interactive technology industries;
- Law enforcement, community policing agencies and school resource officers, legislators, the judicial community and regulatory agencies; and
- Schools and other educational institutions.

Originally formed in 1995 (under another name) to provide help and protection for Internet users of all ages, in recent years, Wiredsafety.org's work has increasingly focused on the safety and good cybercitizenship of children, tweens, and teens. It serves as the umbrella organization for TeenAngels.org, WiredKids.org, WiredCops.org and WiredTeens.org.

WiredSafety.org is dedicated to protecting children in cyberspace from cybercrimes and abuse, including from each other. This involves protecting them from cyberbullying, hacking, sexual harassment and identity (ID) theft. It also includes protecting children everywhere from Internet-related sexual exploitation. WiredSafety.org helps protect them from risks posed by adults, by each other and more recently from themselves, as their reputations and future college and job opportunities are impacted by what they post on their MySpace and other profiles. The package of programs designed for young users with the assistance of our teen and preteen volunteers is called "ThinkB4uClick," teaching them the consequences of their cyberactivities.

Marvel Entertainment, Inc. has also joined forces with WiredSafety.org to provide superhero assistance in educating our children and families on safer online practices. The first Internet safety comic, Internet Super Heroes meet the Internet Villains, teaches how Internet predators can infiltrate anyone's computer and wreck havoc on their lives by stealing their identity and posing as them online. Published under its exclusive license with Marvel, and sponsored by Microsoft, this first comic will help teach the 250,000 readers how to be smarter and safer online using Spider-Man, The Incredible Hulk and Dr. Doom, among others to bring the message to life.

WiredSafety.org also provides information and resources to help educate and guide law enforcement officers on Internet safety issues, crime prevention and investigation of cybercrimes. It has created a special website just for law enforcement officers, Cyberlawenforcement.org, also known as WiredCops.org. As part of the Wiredcops.org initiative, specially trained volunteers assist law enforcement in the investigation and prevention of trafficking of children, child pornography, child molestation, and cyberstalkers. Recently, at the request of leading law enforcement agencies, WiredSafety.org has begun using its teen volunteers to provide information that will assist undercover law enforcement officers in creating credible profiles of preteens and teens to help them become more effective when operating undercover online.

In addition to assisting law enforcement agencies, WiredSafety.org offers one-to-one assistance for victims of cyberabuse that may not arise to the level of a cybercrime and is not handled by law enforcement. WiredSafety's cyberhelpline gives “netizens” access to free help when they need it via the Internet. Its special team of helpline volunteers is assigned to cases and works one-to-one online to help resolve individual problems and get victims help when they need it. WiredSafety.org assists more cases of cyberharassment than any other organization in the world, helping thousands each month through its site and report line. Cyberbullying cases can be reported to the report line as well.

But when dealing with preteens and teens, the challenge has always been getting them engaged. Their "selective hearing" can get in the way of their learning safer and more responsible behavior online, just as it may at home. When approached, teens told us that we had to approach them with things that they consider important, using their language. So, WiredSafety.org recruited teens and preteens who help us do that. These expert Teenangels, 13 to 18 year olds, (and now their younger version, Tweenangels, from 9 - 12 years of age) deliver the message of safe, private, and responsible technology use to their peers. These youth-based programs were formed in 1999 to provide special perspectives and insight into how young people are using the new technologies and how to better prepare them to handle the risks they encounter.

Teenangels have been recognized and honored by Congress, Parliament, John Walsh, Time for Kids and recently, Teen People Magazine, among others. Their training is extensive and takes almost one year to complete. When they receive their "wings", however, they are true experts. It is the only Internet expert youth program in the world. And, once trained, these special teens and tweens help develop safer technologies, by providing expertise for and advising members of the Internet and entertainment industries, media and governmental agencies around the world.

Too often disconnected from the immediate consequences of their actions online, many "good" kids and teens find themselves doing things online they would never dream of doing in real life. This needs to change. The youth programs created by WiredSafety.org focus on cyberwellness and cyberethics which fits perfectly within its mission and expertise. To keep our children safe online, they need to understand the norms and rules of operating online. They must also recognize that they will be held accountable for what they do in cyberspace and that what they post online has ramifications beyond the momentary click. Teaching responsible technology use is crucial.

WiredSafety.org also offers a wide variety of educational and help services to the Internet community at large. Companies such as Disney, the Motion Picture Association of America, the National Sheriff's Association, Yahoo, Verizon Foundation, Marvel Comics, MySpace, Xanga, Johnson & Johnson, Google, Oracle, Facebook, Microsoft and AOL support and turn to Parry Aftab and WiredSafety.org for guidance and advice in dealing with Internet safety issues. Teenangels and Parry have testified before leading governmental and legislative bodies worldwide, including the U.S. Congress and the U.K. Parliament. Regulatory agencies, such as Singapore's Media Development Authority, the U.S. FTC and California's consumer protection arm have sought WiredSafety's and Parry's help. Their collaborative efforts with schools, community organizations, prosecutorial officers, local executive branch and law enforcement agencies, such as Alaska's Campfire USA, the Baltimore County public schools, Ohio's Wayne County Sheriff's office, the San Francisco DA, and Westchester County, NY's County Executive Spano, have affected hundreds of thousands of families worldwide. Using its unique expertise in the field, the charity also assists important trade associations, such as the CTIA (the wireless trade association) and the U.S. Sheriff's Association. WiredSafety.org also acts as a watchdog within most of the social networking websites, to help provide their users safety information and help when things go wrong.

Select volunteers find and review family-friendly Web sites, filtering software products, and Internet services. Some of the outreach team volunteers run programs, summits and also speak at local community groups and schools around the world teaching Internet safety, privacy and responsible use.

However, its work is not limited to the Internet alone. WiredSafety focuses on all aspects of interactive technology use and abuse. Its expertise includes cell phone safety and security, interactive gaming, social networking (mobile and online) and text-messaging products, as well as any new interactive technologies as they are developed. Its long years of working with Internet users and handling cybercrimes and abuse have created a flexible and knowledgeable volunteer force. If you can view content, communicate with others, spend money, or buy things using the technology, WiredSafety.org can help.

WiredSafety.org is headed by Parry Aftab, a mom, international cyberspace privacy and security lawyer and children's advocate. Parry is the author of the first book written for parents about Internet safety - The Parents Guide to the Internet (considered the bible of

online safety and published in 1997) as well as The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000), which has been adapted and translated around the world. Her most recent books have been especially written and adapted for and published in England, China, Spain and Singapore. Her new book, Internet Safety 1-2-3, was released in December 2005 in Spain and will be released next year in the United States. And her new "Stop Cyberbullying!" guide launched in Spain in May 2006.

WiredSafety is proud of its reputation as the one-stop-shop for all cyberspace safety, privacy, security, and help needs. It is even prouder of the fact that all this can be accomplished without large government funding or money wasted on administration costs. No one is paid within WiredSafety.org. They are all unpaid volunteers - including Parry herself. This all-volunteer workforce has been estimated at providing more than $3 million in unpaid services every year. Using a popular website and series of special topic sites, the organization has reached millions of Internet users since its inception and addresses more than 5000 children, teens and tweens and 1000 parents in person every month, on average. WiredSafety.org mobilizes people of all ages who want to help others, and puts them to work doing just that. It is intent on its mission to "Take Back the Net!"

Exhibit B: Parry Aftab's Bio and CV:

Updated July 2006
Parry Aftab

Bio

Parry Aftab is a security, privacy and cyberspace lawyer, as well as an author, columnist and child advocate. A substantial portion of her time is donated to Internet issues involving children, from equitable access, to privacy, to safety, to helping develop quality and reliable content for children. She has also legally represented or acted as a consultant to most of the children's Internet industry, helping them comply with the law, while improving the Internet experience for children. When children and the Internet are concerned, Ms. Aftab's name is the first mentioned.

Parry Aftab is a worldwide leader in the area of online safety and parent and child Internet education. As Executive Director of WiredSafety.org, the oldest and largest online safety and educational program in cyberspace, Ms. Aftab helps prevent and assist law enforcement agencies in investigating cybercrime against children and families. Under its former name, her group was awarded the President's Service Award in October 1998 from the White House and Points of Light Foundation. Ms Aftab also works closely with law enforcement around the world to prevent cybercrimes and police the Internet and is part of the Home Office Cybercrime Task Force in the UK. She was recently appointed a Special Deputy Sheriff by Wayne County, Ohio's Sheriff, Thomas Maurer.

In 1999, Ms. Aftab was appointed by UNESCO to head up its child Internet sexual exploitation project for the U.S. She has also written the leading books for parents on Internet safety since her first book was published on the topic in December 1997.

Although her vocation was Internet security and privacy law, her avocation is children online – helping them become good cybercitizens and keeping them safe, private and secure online. She is dedicated to helping curb Internet-related crimes against children and assisting law enforcement in bringing the child predators to justice. Everyone who encounters Ms. Aftab is impressed with her passion and energy when children’s Internet issues are involved.

While her passion is for protecting children from Internet sexual exploitation, she is also devoted to empowering them through access to the wonders of the Internet. She hopes to help all children become better informed and responsible cybercitizens, controlling the technologies instead of being controlled by them. Her programs are designed to teach them safe, private and responsible technology use, which includes teaching them good netiquette and respect for each other and the rights of others, including intellectual property rights of the music, movie, gaming and software industries.

Ms. Aftab was among the first in the world to devote her talents to keeping children safe online. She has helped design programs for parents and children in a wide range of Internet-related issues for ten years. Her work has been recognized by leading technology influencers, such as Family PC Magazine, when she was awarded Internet Pioneer of the Year in 2001. And child protection agencies have recognized her as well, when Child Abuse Prevention Services presented her with their 20th anniversary Community Leadership Award in 2005. (Past recipients

of this award include Senator Clinton, Linda Fairstein, Judy Collins, Dr. Joyce Brothers and the "God Squad.")

Parry Aftab also provides parent Internet education and online safety content for such diverse sites as Nickelodeon, Children's Television Workshop, Disney, Microsoft, AOL, Yahoo!, Google, AT&T and MSNBC. She is a regular keynote speaker, and resource on camera for the media on diverse cybercrime, safety, privacy and cyberlaw issues. She writes The Privacy Lawyer columnist for Information Week Magazine where she writes on a range of topics that affect technology, policy and privacy. Her expertise is especially in demand on children's Internet issues, because no one knows more about children online than Parry Aftab.

While she is devoted to protecting children online, Ms. Aftab seeks to empower children and their parents, not the censors. Her common sense approach to technology risks and solutions works as well anywhere in the world as it does in the United States. But what really makes her special is her ability to tap into the caring and creativity of young people to craft solutions that are written in their language and designed for their needs.

She is a frequent and respected resource for news programming and print journalists around the world. Her expertise has been featured nationally and internationally in online and print publications, including Readers Digest, Playboy, TV Guide Magazine, Cosmopolitan, People Magazine, Redbook, Biography, USA Today, Information Week, Working Women, Teen People, U.S. News & World Report, Family Circle, Newsweek, Ladies Home Journal, Smart Money Magazine, PC Magazine, Good Housekeeping, Better Homes & Gardens, Family PC Magazine, Yahoo! Internet Life, Information Week, CIO Magazine, The Wall Street Journal, The New York Times, The LA Times, most regional newspapers in the United States, The London Times Magazine, The Strait Times (Singapore), The South China Morning Post Sunday Magazine (Hong Kong), and more. As a result of her work online with children, Ms. Aftab was selected as a charter member of Children Television Workshop's Advisory Board, as well as appointed to The National Urban League's Technology Advisory Committee. In 2003 she was elected to TRUSTe's Board of Directors. She served on the advisory board for the Ad Council for two terms.

Parry Aftab has spoken to many governmental agencies and groups worldwide, conducted briefings for the U.S. Senate, testifies regularly before Congress, and has been a key speaker at the White House Summit on Online Content, the sole Internet-related expert speaking at the 2002 White House summit on Missing and Exploited Children and testified before leading legislative committees and The House of Lords, all with the same message: The Internet is a wonderful resource for families, and once parents understand the online risks, they can use common sense (and perhaps some filtering tools) to help their children enjoy cyberspace safely.

As one of the first lawyers in the world to specialize in Internet legal issues, Parry Aftab is admitted to practice law in New York and New Jersey. She attended law school at NYU School of Law where she received her J.D. degree. She received her B.A. degree as *Valedictorian* of Hunter College (having completed her full undergraduate degree in less than two years), where she was inducted into *Phi Beta Kappa*.

She resides in the New York metropolitan area and is a mother of two. Ms. Aftab can be reached at Parry@Aftab.com.

Parry Aftab

Professional Curriculum Vitae

Phone: 201-463-8663
parry@aftab.com

Internet privacy and security lawyer, licensed to practice law in NY and NJ,
The Privacy Lawyer columnist, author, consultant and public speaker
Executive Director of WiredSafety.org

AREAS OF EXPERTISE: Worldwide Cybercrime Protection and Prevention/Identity Theft/ Privacy, Data Collection and Security / Workplace Risk Management and Security/ Consumer Protection, Advertising and the Internet / E-Commerce/ Cyberstalking and Harassment/ Child Exploitation and Child Pornography, Children Online, Online Marketing, Cyber-workplace issues, Privacy training and coaching

---

CURRENT POSITIONS

President/CEO - Aftab Cyber-Consulting
Executive Director, WiredSafety.org (a 501c-3 corporation)
The Privacy Lawyer columnist for Information Week

EDUCATION

City University of New York — B.A., 1981
Hunter College — *Valedictorian*
(Completed 4 yr degree in 2 yrs) — *Phi Beta Kappa* (Nu Chapter)

New York University — J.D., 1984
School of Law

SELECT HONORS

Community Leadership Award, 2005
Awarded by Child Abuse Prevention Services

American Society of Business Publication Editors Award "Gold" *Original Web Commentary*
Informationweek.com for Parry Aftab's
"Patriotism, Compliance and Confidentiality" article

Activist of the Year Award, 2002
Awarded by Media Ecology Association

Internet Pioneer of the Year, 2001
Awarded by Family PC Magazine

Home Office, U.K.
Child Protection, Criminal Laws and Law Enforcement Task Forces

ORGANIZATIONS

TRUSTe
Member- Board of Directors (Elected December 2002)

Ad Council
Advisory Committee member (1999 - 2003)

Children's Television Workshop Online (Sesame Workshop)
Advisory Board (1998 – present)

UNESCO
President, U.S. National Action Committee, Innocence in Danger (appointed 1999)1998-present)

The Internet Society
Elected Chair, Internet Societal Task Force and Societal Steering Group (worldwide, 2001)
Member of Public Policy Committee ISOC (2001–present)
Chair, Privacy and Security Working Group of The Internet Society Task Force (2000-2001) appointed member since 1999

WiredSafety (wiredsafety.org) the world's largest Internet safety and help group, formerly functioned as "Cyberangels," recipient of President's Service Award, 1998,
Executive Director (1998-present)

The National Urban League
Technology Advisory Committee (1997 – present)

AUTHORSHIPS AND
RELATED ACTIVITIES

Author, selected books

Cyberbullying Guide (Spanish and English guide on preventing and dealing with cyberbullying)
Spain 2006

Internet con los menores Riesgos (Spanish guide for parents on Internet safety, especially written for Spain and South and Central America)
Spain 2005

Children and the Internet (official Chinese Internet safety guide)
China 2004

The Parent's Guide to Protecting Your Children in Cyberspace, McGraw-Hill, (U.S. edition, January 2000; UK edition, March 2000; Singapore edition May 2000 and Spanish language US edition November 2000)

A Parents' Guide to the Internet, SC Press (October 1997)

Contributor, selected books

Child Abuse on the Internet.... Ending the Silence
(2001) Carlos A. Arnaldo, Editor
Chapter 21: The Technical Response: Blocking, Filtering And Rating The Internet - by Parry Aftab

The Best In E-Commerce Law
(2001) Warren E. Agin, Editor
Children's Online Privacy Law

Selected Speaking Engagements

WiredSafety's Social Networking Summit, June 2006

US Congress, Commerce Committee, Sub-Committee Investigations and Oversight, opening day hearings April 4, 2006

National Association of Independent School Annual Conference, March 2006

Stonybrook Cyberbullying Summit, September 2005

FDIC Conference on Security Online, August 2005

The Westchester County Cyberbullying Summit, February 8, 2005

The US Copyright Office – Luncheon Speaker (LA and SF events) February 2005

Child Abuse Prevention Service 20th Anniversary Luncheon Speaker, April 2005

FTC Workshop on P2P, December 2004

House of Commons – Parliamentary Briefing on Internet Safety, October 2004

IAPP (International Association of Privacy Professionals), June 11, 2004

EU- Safer Internet – Warsaw, March 2004

Media Development Authority- Singapore, Family Internet Week – March 15, 2004

Western Attorneys General Conference, July 29, 2003

Domain Day, Milan, Italy, November 5th, 2002

Wired Kids Summit, Washington D.C., October 15th, 2002 (Mediator and Host of the event at the Russell Senate Building)

White House Conference on Missing and Exploited Children, October 2nd, 2002 (Only panel speaker selected to discuss Internet issues). Other speakers included President George W. Bush, Colin Powell, John Ashcroft, Rod Paige and many distinguished others.

Council of Europe, Children's Online Safety, Belgium, November 2001

Microsoft, Privacy and Security Summit, Privacy Speaker, San Francisco, November 2001

Intellectual Property Organization, Featured Speaker on Internet Law, Privacy and Digital Rights, New York, November, 2001

SCOPE, Keynote Speaker, Cyber-terrorism, New York, October 2001

Rappateour, E.U. Online Content Regulation, Luxembourg, June 2001

Bertelsmann Foundation, Experts Meeting, Singapore, February 2001

Microsoft, Privacy and Security Summit, Speaker (only female speaker), Seattle, November 2000

Keynote Speaker, House of Lords, Kids Helping Kids, London (April 2000)

Keynote Speaker, Singapore Broadcasting Authority and Ministry of Information Conference, Children Online, Regulatory Issues, Singapore (November 1999, May 2000, February 2001)

Panelist, FTC Hearings on COPPA Regulations, Washington (June 1999)

Keynote Speaker, White House Summit, Online Content, Los Angeles (June 1998)

Keynote Speaker, C.A.R.U., Conference On Children's Online Privacy
(September 1998)

Featured Speaker, Littleton Town Meeting hosted by Tom Brokaw and Jane Pauley, MSNBC (April 1999)

APPENDIXES:

Appendix 1:

Parry's Info for Parents...What are our kids doing online?

Know that our kids doing things online that we would freak if we knew about isn't new. Our kids have been saying and doing outrageous things online since the Web was born. We just didn't know about it, but all the other kids do. It's how they communicate online. In 1999 we conducted the largest academic survey done to date for teenage girls. Almost 11,000 of the teens polled answered our questions about what they did online. When we asked them to explain if they had done anything online that they wouldn't have done in person, here's what they said (in their own words):

- "Yes, obviously people are more bold and outgoing on the Internet when they don't have to deal with the consequences of their actions."
- "Of course! All people do. A computer with a phone line is like a mask to the world. You can do or say anything and you won't ever have to meet this person. For instance, my little brother is 13 and he tells people he's 16 or older. He's a sweet guy and has a very high respect for females. Online, however, he says very cruel and suggestive things to and about them. He acts like a monster. It's disgraceful... and a little scary."
- "Yes, of course... our usual boundaries and personal walls are down and we can act more carefree and outspoken if we feel like. At least this is true for me... you can act like a goddess."
- "I have cursed out a lot of ppl [people], and when my bud comes over, we go into places like the African American room and yell "KKK ALL THE WAY" or go to the Jewish room and say "HEIL HITLER," but I haven't done that since I started going back to church and was saved by Jesus Christ. We were just joking, we weren't really racist."
- "Yes, but I'd rather not describe what I did. Instead, I'll just say that online, you can be absolutely ANYONE you want to be, which is why a lot of people do things that they would not normally do. In real life, people everywhere judge you based on your looks, actions, and who knows what else, but online, all that really matters is your attitude and personality."
- "Uh well, I tried cyber sex before and I wouldn't ever do that in real life. Sex period. I don't believe in premarital sex. I think that is a great gift you give your husband. I once told someone off because he/she was being perverted and talking nasty to me and I didn't like it."
- "Well, once I told this guy I met in a chat room all about me and, like, my phone number and stuff. I now realize that this was really stupid of me and will never do anything like it again cause although it's not likely, he could be a psycho or something."
- "I feel I can speak more freely to someone online about my problems because most of them don't go to my school or even the same state. I can ask them advice and they would probably give me the best because they aren't in favor of a certain person. I can introduce myself and meet new people because it isn't as uncomfortable to look into their eyes and if you become really uncomfortable I can just get out of it by blocking them or getting offline."
- "I have had cyber sex... that's something I never have done and never will do until I'm married in real life."
- "I am much more bold online than in real life. I am VERY shy and I say things on the Internet that I normally wouldn't say in public."
- "I have lied for no reason. Actually, I told a guy I couldn't give him my number cause my mom doesn't want guys calling me cause it was during the school year. My mom

doesn't really care who calls me I just didn't know what to say."

- "Yeah, I wouldn't flirt with people I just met in person, unlike on the Internet."
- "Flirt more easily, say things I wouldn't say in person, not bad things, just more honest things."
- "Yeah, because it's a lot easier to talk and get to 'know' someone online because you can't see their face. I never have done anything bad but I've been a lot more easy going and free for what I'd say online then in a live situation which in someways have helped me to be more comfortable talking to new guys in person."
- "Well, honestly... yes. I had cyber sex! I will never have real sex until I am married, after I engaged in cybering, I totally felt grossed out, like I know I was doing something wrong! I will not make that mistake again."

When we asked them if they ever pretend to be someone else in cyberspace, here's what they answered (in their own words):

- "Of course I've pretended. Everyone does. You pretend to be older... or you pretend to be a guy... or you just pretend to be whoever you wanna be."
- "Yes, I just changed myself to be someone I wasn't because I wanted to get a different reaction from people. It gave me a way to see myself as who I wanted to be but by doing it I realized that that is not who I want to be and that I just want to be me."
- "Yes. If I am ever in a chatroom I always make up things about myself. This is why I say don't trust anyone because everybody else does the same thing."
- "Since nobody seems to be eager to talk to a 15 year old, I always pretended I was 18 year old female. However, that sometimes attracted bad attention from guys."
- "Yes. I pretended to be anyone from Leonardo DiCaprio to a serial killer."
- "I once pretended to be a 16 year old girl. I wanted to talk to my boyfriend to see if he would agree to meet her in person. He did and I told him who I really was and we broke up."
- "Yes, I've pretended to be so many people. It's fun and safe and because nobody knows who you really are."
- "Well we've ALL pretended to be older or have a different name or something. Who doesn't? It's part of the fun about being online... you can be whoever you want to be for a little while."
- "Yes, I pretended to be someone that I wish I could be like a popular person."
- "I haven't pretended to be someone else, but I have pretended to be a couple of years older than I am, because not many people my age are online to talk to, and if they are, they must be lying about their age, too."
- "No, I think it is wrong to lie to other people about who you are. I wouldn't want someone to do it to me so I don't do it to them."

When we asked them if they had ever been in a situation online that frightened them, here's what they said:

- "My friend agreed to meet a guy she met online when he came to our hometown, and she wanted some of us to come along to keep them company. I told my parents but luckily the guy's game got canceled. I wouldn't have gone and I would not support her decision to meet anyone in real life. She kinda felt betrayed but at least she's still alive."
- "Once I was scared because this guy kept telling me all this stuff about me, like my name, address, friends' names, etc. he said he knew where I lived and stuff, and I better watch out. It ended up being a joke from a friend of a friend, but I was still scared, and I was very angry at the friend who gave the person the info just to scare me. It wasn't funny."
- "Once I was on ICQ talking to a bunch of my friends when this guy I had been chatting

with sent me a file. Unknowingly, I opened it and then I realized that the person had hacked into my system. Suddenly, my CD-ROM drive started opening and closing and annoying (but not threatening) messages started appearing on my screen. Soon after my mouse buttons switched functions. I had just finished a big assignment, so I was afraid the hacker would do something to wreck it. I shut down my computer and that was about all I did about it. One of my friends had a similar experience, only hers was scary and threatening. When she got hacked, pictures of a dead girl with her face smashed in appeared on her screen, along with threatening messages and sound clips."

- "I know this is normal in fact it doesn't bother me I just laugh. Most kids are always exposed to this stuff not just on the Internet so its no big deal in fact sometimes it makes it interesting. But one time this dude got really mad at me and he knew my parents were out of the state and he could have called one of my friends and found my address but instead he kept calling every 5 minutes...."
- "There was one time, when I got online to check my e-mail. I ended up going into my regular chatroom, and when I arrived, some guy started giving out my personal information. I don't know how he knew anything personal about me, but he was telling everyone in there about the frightening and terrible things that were done to me as a child. My best friend doesn't even know what happened to me when I was little. All I did was, denied all of what he said and logged off. I cried all week long."
- "This guy IM'd [instant messaged] me and my best friend and he knew all this information about us... and we hadn't even talked to him before. He knew who we were, where we lived and everything and he kept playing with our minds trying to tell us that we started IMing him first and so on. I told my parents about it but they didn't really care. So this went on for an hour and a half. I had friends try to get him to stop. He told us where he worked and he kept insisting that we go places with him like out to lunch or dinner and he would buy us x-mas and b-day presents even though we had never met him. He would leave them on his car at work for us to come and get, we would go get them and just smash them all over the ground... thinking he would get the point. He was convinced that him and my best friend were dating then I came along and I'm the one who stopped it all. No one could get this guy to stop. We changed our screen names plenty of times but he had already hacked into our account so he could always find us. Well he hacked into mine. Well in December we got a new computer and we both changed our screen names and he hasn't been able to find us since."
- "[A]bout a year ago I met a guy online and I told him my phone # and found out he lived about 5 minutes away from me we talked 4 about a week then he asked me out and I agreed. We met up at the mall he was totally normal 15 year old guy. He wasn't some psycho or anything but I got in a lot of trouble from my parents and I will never give out any personal information again. It's not safe and its a stupid idea. If anyone who reads this is thinking about giving out info to someone on the net PLEASE think twice about it you could get yourself into a lot of trouble."
- "I received a threatening E-mail from someone on my E-mail address. I immediately changed my password, and made sure that I didn't have information on my profile. I never E-mailed the person back, since that is what lets them know your account is active and they can find out more about you. Then, I decided to make sure about it, and stopped checking my E-mail account. I just got a new one."
- "I was in a chat room once and this person was threatening to kill themselves, and I find that scary. So I IM'd them not to do it, and I chatted with them for a while, and made them feel better about themselves, and promise not to do anything drastic. And they did promise."
- "I told these people to leave this foreign guy alone because they were making fun of him. They were calling him names and mocking everything he said. The people I got

smart with told me I better watch my back because they could find out where I lived. That's why I left."

It would be interesting to ask your children to reply to the same questions. You might learn something about your children you didn't know.

Appendix 2:

The Quick Tips on Keeping Our Kids Safe on Social Networks

The quick tips for teens:

- Put everything behind password protected walls, where only friends can see
- Protect your password and make sure you really know who someone is before you allow them onto your friends list
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators
- Don't post anything your parents, principal or a predator couldn't see
- What you post online stays online - forever!!!! So thinkb4uClick!
- Choose a network that lets you control your own security settings and who can see what you post.
- Don't so or say anything online you wouldn't say offline
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their pic online
- Check what your friends are posting/saying about you. That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!

And for parents:

- Talk to your kids
- Don't panic
- Be involved
- This too will pass!

For help or more information, visit WiredSafety.org.

Appendix 3:

Wireless Safety...Keeping Your Kids Safe Using Cellphones and Other Mobile Devices

You've already heard the tips about keeping your kids safe online. But, now...all bets are off. Welcome to the wonderful new world of wireless! Our families can carry powerful computing in handheld devices the size of a pack of playing cards (or smaller!). They can download and play music, movies, and games. They can shoot, store and share photos, video and audio. They are always in touch, always connected, always engaged. (And the newest hottest teen social network, Yfly.com, is using broadcast text-messaging to keep teens connected to their nearest and dearest friends to through their mobile devices too and MySpace and Facebook are using text-to-profile posting technologies now too.)

Great! Except the most often repeated safety tip warns parents to keep the computer in a central location to keep an eye on what's going on. So, how are we supposed to keep our kids safe when they are carrying access and communication devices in the palms of their little hands? Are we supposed to tell them to keep their cell phone or other handheld device in a central location? Of course not. At this point, it's less about standing over their shoulders and more about improving the "filter between their ears."

You can do this by being proactive and informed (not rocket scientists, just informed...). Luckily, it all comes down to 3 key issues. I call these the "3C's" – Communication, Content, and Commercialism. Every digital device or interactive service involves at least one of them, some involve all 3. Once you find the Cs involved, spotting the risks and solutions is easy.

Start by reviewing all your interactive technology devices and services. If you are shopping for a new device or service, ask the salesperson these questions before plunking down your hard-earned money.

- Communication: Does this device or service allow you to communicate with others? Does it allow others to communicate with you? If so, how? What controls exist to block, filter or monitor these communications? How can I implement them? (Text-messaging and voice capabilities fall into the first "C". So do e-mail, interactive features on profiles, and on blogs.)

- Content: What content or images can be accessed or shared using the device or service? Can you surf the Web, access blog or profile sites, post your blog or profile sites or download media? Can you store images, personal information, video, songs, etc? What controls exist to rate, block, filter or monitor the content? How can I implement them? (Music and video downloads, pictures taken by the mobile device, adult content, content on profiles and on blogs fall into this second "C".)

- Commercialism: Can this device/service cost me money? If so, how? Are their ways to spend money or buy things using the device / service? Are their ways to control costs or prevent my kids from spending money or buying things without my approval? What controls exist to block, filter or monitor these costs or spending ability? How can I

implement them? (Ringtones, music downloads, text-messaging and games fall into this third C.)

Next, you need to refer to the common sense tips our grandmothers taught our parents and they taught us --we just need to translate them from "Grandma-speak" to "cyberspeak."

Don't talk to strangers.

It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace, or on text-messaging. Our kids need to learn that unless they know the people in real life ("RL"), the person has to be treated like a stranger no matter how long they have chatted online. Period.

Come straight home after school.

When kids wander around, unsupervised, after school they inevitably get into trouble. Allowing your children to spend unlimited time surfing or texting aimlessly is no different. Set a time limit. Create a "no texting" zone, where they spend time with their real life friends and engaging in family activities (and homework).

Don't steal.
Illegal music, movie and game downloads. Enough said!

Don't start fights.

Cyberbullying is when one minor uses interactive technology to harass, frighten or humiliate another minor. They may even spread into RL. Our children should be taught to Stop (don't do anything to make matters worse), Block (the offender) and Tell (you or another trusted adult). (You can learn more about this at stopcyberbullying.org.)

Don’t take candy from strangers.

While we don’t take candy from people online, we do often accept attachments. A seemingly innocent attachment can contain a virus, spyware or a hacking tool. Many of the good anti-virus programs have mobile versions. They are worth the investment.

Don't share personal information with others.

Our children often post their cell number on their instant messaging "away page." Mobile device cameras can be used to take a picture and post it online. Make sure your children understand what can and cannot be shared. Remember...The more information you give your children, the less information they'll give a stranger.

Look before they leap.

Check things out before your child starts using a new interactive device or technology or activity. Let them know what features you don’t want them using and which ones are safe. And remind them that you will be watching. This is a matter of parental choice and control. The wireless industry is providing some significant help here too. They have voluntarily adopted a set of principles relating to mobile content provided by the carriers themselves, rating them as "restricted" (for those over the age of 18). Restricted content is only available with authentication, allowing parents stay in control. Disney has a new cell phone service and phones launching in June, 2006 too. (Visit disneymobile.com and ctia.org for more information.)

Do unto others as you would have them do unto you.

It is too easy for our children to act out online knowing that they may never have to face the other person in real life. Not having to look them in the eyes makes it easier to be rude, lewd or hostile. This is a good time to remind your children to treat others online and off with R-E-S-P-E-C-T.

Now...go have some fun and play a little! And if you are still tech-challenged, ask your kids for help.

And for more cybersafety tips and help or to book a program for your community, visit WiredSafety.org, the world's largest Internet and wireless safety and help group or contact Parry Aftab directly at parry@wiredsafety.org.

Appendix 4:

Parry's Social Networking Advice for Parents:

It's worth the effort to find out if your child is one of the social networks. Start by asking them. Hopefully they will be honest with you. If they aren't or you suspect they may be lying, it doesn't hurt to check out the more popular ones yourself. Search for your child by e-mail address, name and school. While they often lie about their e-mail address (either creating a special free web-based one just for this, that you may not recognize, or by making one up) or their name, they NEVER lie about their school. That's the only way their friends can find them. If you discover that your child has one of these profiles (or several, which is very common) and is lying to you, you need to take action. This isn't about technology, it's about dishonesty and hiding something important from you. And it might be a good time to buy and install a monitoring product, to be able to find their other lies and their next social-networking website they are trying to keep you from seeing.

If they admit that they have a page and show it to you, review it carefully, without over-reacting. Keep an open mind. (And take 5! To keep from panicking!) Have they posed as someone older? Posted person images? Included their friends on their site or been included by their friends on their sites? Forget the language. It's what kids do online. Caution them, but don't judge them by the language they use online. If they are posting using chatlingo shorthand, you can visit Teenangels.org and use our chatlingo translator to see what they are saying.

Then you have two choices. You can have the site taken down, or you can supervise what they are posting and doing. It's important hat you help keep your child safe online, even if you may be shocked by what you find your child is saying behind your back. And be aware that these are important to them. They all do it, even if they shouldn't. So, it's possible that your young teen will rebel and just set up a page again, but hide it better this time. It may be better to work with them than prohibit the profiles altogether.

Next, don't panic. You should take advantage of this opportunity to review their page first. You might be surprised (hopefully pleasantly) by what they are saying.

If they haven't posted anything to put them at risk, and aren't communicating with strangers, ask them why they want a social-networking profile page. You might be surprised at what they tell you. While parents freak out (understandably) at the provocative images and wild language used by many on these sites, most of the teens don't see them or pay attention to them. They are there to show off their creativity and self-expression and to communicate with their offline friends. As long as they are old enough to understand the rules and adhere to them (no one under 13 is old enough for this, even with parental approval in my humble opinion), and as long as you keep an eye on what they are doing, posting and how they are communicating with others, it's YOUR choice as to whether they keep their site up or not. (Make sure that you don't become the self-appointed profile site, reporting other people's kids for posting underage until you speak with their parents first!)

If you find that they are saying and posting inappropriate things or those comments don't seem to conform to their otherwise good offline behavior, don't panic yet. Think about

how our parents would have reacted if they could have seen or heard everything we said to our friends when no adult was around. I guarantee that they would have been almost as shocked as many parents are about what their kids are posting online.

Also, remember that many of the things your kids are saying are being said to impress their audience and are often not true. (Luckily!)

The important difference between what we used to say or do and their posting online, however, is that when we acted out or boasted about acting out, we didn’t do it to an audience of millions of people. So, while you shouldn’t panic, you should take quick action if your kids are posting personal information in a public forum, or communicating with strangers online.

Now repeat after me..."I am the parent!"

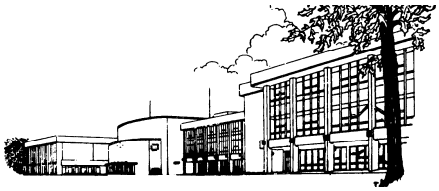
Appendix 5: How schools are handling these issues

A letter for parents from a school, using Parry's tips:

LAKEWOOD HIGH SCHOOL
14100 FRANKLIN BOULEVARD LAKEWOOD, OH 44107

Voice: (216) 529-4028 Fax: (216) 529-4459

Web: HTTP://WWW.LNOCA.ORG/LAKEWOOD/LHS/



Dear Parents/Guardians:

Many of you are aware of the popular websites used by teenagers for blogging and socializing, such as MySpace.com. Recently, our staff has become aware of inappropriate content that many of our students are posting on these public websites. This letter is being sent to inform you of these websites and to encourage you to talk to your child about internet safety and appropriate postings. The following information is provided by Parry Aftab, cyberspace lawyer and executive director of WiredSafety.org, the world's largest Internet safety and help group and taken from her safety tips published at MySpace.com with her permission.

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. Sometimes people do this to find romance. Sometimes they do it to find friends with similar interest. While this may be okay for adults, it is not okay for kids.

MySpace.com recognizes this, and prohibits anyone under 14 years of age from using their website. Unfortunately, while they may set rules to keep younger kids off the site, they can't prevent kids from lying about their age, pretending to be 14 years of age or older. To address this, MySpace.com has developed special software to review the profiles of their members, to try and find anyone under age, based on information the members post about themselves. It's not perfect, but it does help spot many underage members.

While MySpace.com is doing its best to keep your children from using their website and lying about their age, it's up to parents to do their job too. Parents need to talk with their children about not sharing personal information online. Personal information includes pictures, names and addresses, schools they attend, cell and phone numbers and many other less obvious things, such as the name of their school team, ethnic background and even a mall near your house. (You can learn more about how to talk to your kids and what you should be asking at WiredKids.org or WiredSafety.org. I am an Internet privacy and security lawyer and founded the all-volunteer Wired Safety Group. We can help you if

things go wrong online, or you just have questions. We provide information, education and one-to-one help for victims of cyberabuse.)

We at WiredSafety.org are developing a special program just for parents concerned about their kids using social-networking and online dating sites. It will teach you what you need to know about finding out if your child has a profile on one of these sites, how to review them and remove them, if you want to. It will also help you if your child is being cyberbullied using one of these sites or members from these sites, or is cyberbullying others.

So what do you, as a parent, do? First you need to find out if your child has a page on one of these sites. The best way to find out if your child has a profile on this or another similar site is to ask them. If you're not sure that your child is being honest with you, you can search MySpace.com (or the other sites) using their e-mail address, or by searching for their school. (You click on "search" and enter their email address or full name in the appropriate search box.)

If you find that your child has a profile on the Web site, you should review it. It's amazing how much you can learn about your child by reading their profiles. Does it contain personal information, such as their full name, address or phone numbers? Has your child posted photos? Are they photos of themselves or someone else? Are they sharing poems they write or provocative comments about themselves or others?

If you want the profile removed (you must remove your child's profile if they are under age), first ask your child to remove it themselves. If that doesn't work, MySpace.com has a section explaining how to remove a page. If you find someone who is underage, you can report it there as well. It's not as easy a procedure as the other Web sites.

While MySpace.com is working hard to keep kids off their Web site, ultimately, protecting your child is your job. But you have lots of help. At WiredKids.org and WiredSafety.org thousands of volunteers donate their time to helping parents and children surf responsibly and safely. And we will be building a few tutorials help parents and their children understand how to be careful when communicating publicly online.

A good thing to do is to ask your kids why they created the profile. You might learn that they wanted to share their thoughts with others, make new friends or even allow others in their school to get to know them better. But not all of their motives are as noble or safe. Some may be interested in meeting new romantic interests or role-playing inappropriately online. And when a young preteen lies about their age posing as a seventeen year old at the site, that can be a serious problem. Others in their late teens might approach your child thinking they were older. That's bad for everyone.

If you discover that your child is posting provocative comments or inappropriate images online, it's time for the tough talk. The one about stranger dangers and how that cute fourteen year old boy they meet online may not be cute, may not be fourteen and may not be a boy. (Parents of young boys need to understand that their children are equally at risk. About one-third of the cases of Internet sexual exploitation are men exploiting boys.) Our children need to realize that there are real risks relating to meeting strangers offline, including murder.

It's not easy raising children anymore. It is even harder when the parent is expected to be expert in Internet, cell phone and interactive game risks. The good thing is that you're not facing these challenges alone. We're here to help.

Just remember that while your kids may know more than you do about technology, you know more about life. And you are allowed to set the rules and enforce them. You're still the parent! There is software you can install that will record what your kids say and post online. There is even one that will e-mail you reports at work. The ones I like best are made by Spectorsoft, and can be found at software4parents.com or spectorsoft.com. But don't use them just to spy on your kids. Treat them like a security video camera in the corner of a bank. No one views the tapes unless and until there is a break-in. Do the same here. Check the program reports if something goes wrong. It will collect whatever you need for evidence and to help your child if something goes wrong.

Also, check your parental control programs. Many, such as AOL's and MSN's, can block access to social-networking Web sites or other sites you think are inappropriate for your younger child. There are many other products you can purchase to block sites as well. (Check out software4parents.com to learn about and purchase some of these.) Just remember that the best filter is the one between your children's ears.

Please feel free to contact your child's counselor or house principal if you have any concerns. And visit Parry's cybersafety blog and podcast, http://parryaftab.blogspot.com, and WiredSafety.org for more tips on cybersafety and social networking issues.

A principal's letter to the parents of his students:

I know that history repeats itself and some things never change and there is nothing new under the sun, etc, etc, etc. Having spent so many years in school buildings, I really understand how much truth there is to these clichés. From the first day I started working in schools more than 38 years ago, I have been involved in helping young people deal with the consequences of making poor decisions involving things like drugs, alcohol, vandalism, theft, bullying, etc. It will always be this way and that is part of the job of teachers and administrators in public schools.

It can come as no surprise to anyone reading this that drinking is rampant among many of our students almost every weekend. Drinking to excess (bingeing) is now more common than ever before. Is it watching MTV Spring Break year after year that has caused this new form of excess to be so common? I don't know. I do know that our kids do it, and do it often.

I'm sure everyone knows at some level that to smoke, or snort, or ingest, or inject drugs costs lots of money. How do our kids who choose to engage in this kind of behavior get the money to sustain it? It is either provided to them by way of an allowance or bank card, OR it becomes available in other ways…..theft, sale of personal items, providing services of some kind, etc. We all know enough about drugs either through reading, watching movies, or hearsay, to know that no one provides a sustained supply of drugs to someone else out of the goodness of their hearts. They want something in return. How do our kids get access?

Bullying used to be relegated to the big, tall, tough guy/gal in school. After all, it took muscle and might to back up those words and deeds. Now, through e-mail, instant messages, text messages, the phone, personal home pages, etc. just about anyone can bully someone else and remain anonymous. The 98 pound weakling no longer has to bulk up to be a bully. She/he can do it from the privacy of the bedroom and remain at that weight.

Here is what has really changed. Personal home pages are now almost the norm among our young people with access to computers and broadband Internet service. You would be shocked and surprised to visit some of the home pages of our middle school and high school students. Some of the information they share about themselves is embarrassingly personal, graphic, and explicit, AND it comes with names, addresses, and phone numbers. In truth, most of these kids think they are setting up a page that they and only their close friends have access to. In truth, just about anyone with a real facility with computers can find these sites and pick someone who interests them to prey upon.

I am sharing this disturbing information with you because we all worry about your/our children. Most, if not all of this activity, takes place at home or at someone else's home. If it took place in school, we would have a record and would track it. There are consequences for this kind of behavior at school using school machines and our Internet service. When it happens from elsewhere, we have no control over it. I don't even know how **you** can control it. I simply want the piece of mind knowing that I have shared this with you. It is epidemic among our young people and opens the door for unimaginable problems for them and for YOU, their parents.

I rarely write or speak about problems for which I have few or no solutions. I can't even suggest a solution other than to be vigilant and to know it is going on, if not at your home with your child then with your child's best friend or your neighbor's child. Let's bring this topic into the open and start talking about it whenever groups of adults gather for whatever purpose. Our children need to know that we know what is going on. It is dangerous and they are too young to understand. If you can think of something that would be helpful to parents and you plan on attending the next evening "coffee" in March, please share it with me and I will pass it along to other parents via e-mail or this Newsletter.

Appendix 6:

Parry's Myspace Guidebook Table of Contents

(the guide will be released for back to school without charge at WiredSafety.org)

1- **Introduction to Myspace**
a. Origins/History
b. Why people use it
c. Basic ideas of how Myspace works
d. Explaining the ‘cyber friends’ process
e. Pitfalls of chatting online
f. Reasons to use social networks

2- **Getting started**
a. Creating your homepage
b. Uploading images/Using appropriate images
c. Content- not revealing too much personal information
d. Settings, and controlling ‘Friends’ lists
e. Finding others with similar interests, in your area or at your school
f. Using Myspace to network
g. Searching for specific people on Myspace
h. Creating and using an avatar
i. Privacy settings
j. Younger profiles settings (between 14 and 16)
k. Reporting abuse
l. Getting help
m. Pics, quizzes and getting codes from third party sites

3- Writing a profile
a. Creativity-expressing yourself through a blog/profile
b. Blog/profile ideas, like a diary, it can be a journal of your thoughts
c. Writing with some caution-not revealing detailed information
d. Reading and contributing to other members blogs/profiles

4- Hazards of meeting people from the Internet in real life
a. Using caution when replying to e-mails and communications from strangers
b. Unsolicited contact, using judgment to better safeguard yourself
c. Meeting people face to face offline
d. "You never know..." how even smart teens and preteens are tricked by posers
e. You don't have to meet them offline to be sexually exploited - webcams, cybering and child pornography

5- Risks from adults, from other teens and risks you pose to yourself
a. Sexual exploitation issues
b. Cyberbullying, stalking and harassment
c. Protecting your reputation online
d. What employers, colleges and police are doing on social networks
e. ID theft, scams and posing
f. Protecting your passwords and personal information

g. Protecting your personal information - when your friends post your info

6- What you need to know to keep yourself safer

a. Having fun on Myspace, safely
b. Using good judgment to identify potential dangers
c. Using creativity to express yourself through blogs/profiles
d. Letting an adult know if something happens
e. Talking to parents/adults about people you meet online
f. Using extra caution when sharing images or chatting
g. Talking to friends about safety - protecting yourself and your friends online

Appendix 7:

Parry Aftab's Guide to Keeping Your Kids Safe Online

MySpace, Facebook and Xanga, Oh! My!

Keeping yourself and your kids safe on social networks

The quick tips for teens:

- Put everything behind password protected walls, where only friends can see
- Protect your password and make sure you really know who someone is before you allow them onto your friends list
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators
- Don't post anything your parents, principal or a predator couldn't see
- What you post online stays online - forever!!!! So thinkb4uClick!
- Don't so or say anything online you wouldn't say offline
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their pic online
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!
- And, unless you're prepared to attach your MySpace to your college/job/internship/scholarship or sports team application…don't post it publicly!

And for parents:

- Talk to your kids – ask questions (and then confirm to make sure they are telling you the truth!)
- Ask to see their profile page (for the first time)…tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe…and it becomes a way to teach them what not to post instead of being a gotcha moment! Think of it as the loud announcement before walking downstairs to a teen party you're hosting.)
- Don't panic…there are ways of keeping your kids safe online. It's easier than you think!
- Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did that your parents would have killed you had they known, when you were fifteen.
- This too will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts and get help when you need it. (You can reach out to WiredSafety.org.)
- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock drawer…and reading their MySpace. One is between them and the paper it's written on; the other

between them and 700 million people online!

- Don’t believe everything you read online – especially if your teens posts it on her MySpace!
- And, finally….repeat after me – “I’m still the parent!” If they don’t listen or follow your rules, unplug the computer…the walk to the library will do them good. ☺

Appendix 8:

SNAPSHOT OF U.S. MINORS ONLINE AND HOW PREDATORS REACH THEM

(Taken from Parry Aftab's testimony before the House Sub-Committee on Investigations and Oversight on April 4, 2006)

It is estimated that approximately 75 million minors in the Unites States access the Internet either from home, schools, community centers and libraries or from some newer Internet-capable device. This is up more than ten-fold since 1996, when only 6 million U.S. minors were online. Now our children are using cell phones with Internet and text-capability, interactive gaming devices (such as X-Box Live and Sony Playstation Network) with voice over Internet and live chat features, handheld devices with Bluetooth and other remote-communication technology (such as PSP gaming devices and mobile phones) and social networking profiles (such as MySpace, Facebook, Bebo, YFly and others) where they can advertise their favorite things, where they live and pictures of themselves and their friends to anyone who wants to see them.

Ten years ago, when I first wrote my safety tips telling parents to put the computer in a central location, that made sense. It was a central point, where parents could get involved and supervise their children's interactive communications and surfing activities. Now, where they take their communication technologies with them in their pockets, backpacks, and purses, it is not longer as relevant as it once was. Now, instead of expecting parents to watch everything their children are doing online from the comfort of their familyrooms, or kitchen counter, we have to do more. Now, we have to teach our children to use the "filter between their ears" and exercise good judgment and care when using any interactive device. While teaching parents how to supervise their children online was a challenge (I have written the leading books, worldwide, for parents on Internet safety), teaching children to "ThinkB4uClick" is much harder.

When I was growing up (in the days before electricity and indoor plumbing, when we had to walk up hill, both ways!, in blizzards to get to school), parents used to blame us for not behaving. We were disciplinary problems. Now pediatric neuro-psychologists tell us that preteens and young teens are hardwired, through immature brain development, to be unable to control their impulses at this age. Either way, we recognize that preteens and teens take risks, don't appreciate the consequences of their actions and act before they think. When their audience was their school friends, family and neighbors, the risks were containable. When they act out where 700 million Internet users can see, it takes on a much deeper significance.

Putting Their Heads into the Lion's Mouth

Now, I will share something very controversial. While educators and child psychologists understand this, most parents will be shocked at the suggestion that their preteens and teens are in control of their safety online and putting themselves at risk, often intentionally. But unless we accept this, and direct our attentions at solutions aimed at this reality, we are all wasting our time. We will focus on the much smaller segments of preteens and teens who are being victimized through not fault of their own - those who

are targeted at random. All others need to change their online behaviors. And that's where we need to devote all our attentions.

For this to happen, you need to understand the truth. For years we have told parents and minors not to share too much personal information online. "You can be tracked down in real life," we told them. But, notwithstanding anything to the contrary reported in the media and by some local law enforcement officers, to my knowledge, to this date, no preteen or teen has been sexually-exploited by someone who tracked them down from information they posted online. In each and every case, to my knowledge, to teens and preteens have gone willingly to meet their molester. They may have thought they were meeting someone other than the 46 year old who is posing as a teen, but they knew they didn't know this person in real life. They are willingly agreeing to meet strangers offline.

What does this mean? It means we can do something about this. It means we can educate teens and preteens about the realities of meeting people in real life they only know in cyberspace. It means we can create solutions. It means that this is, at least for the time being, 100% preventable. It means that what we do today will have an immediate impact on the safety of our youth. It means we have to join together and work on things that are effective and abandon those that are not.

But we have to act quickly. When I testified before the U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000, I cautioned:

Law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. But it’s only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes. (See Testimony of Parry Aftab, Esq. U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000.)

Luckily, while our young people are sharing much more information online than ever before, to my knowledge, predators aren't using it to hunt down our children offline. They are like vampires. They need to be invited in. Sadly, our teens and preteens are too often doing just that. They are inviting them to offline meetings, phone calls and videochats. But, as an expert in cyberrisk management, I can tell you that this is good news. Because we have a single point of risk - our children, preteens and teens. If we stop their risky and unsafe behaviors, and teach them when to reach out for help, we can manage this risk. We can keep our children safe.

Our children are mainly at risk because of their own actions. Some are intentional. Others are inadvertent. They may willingly engage in communications with people they don't know in real life "RL," agree to meet them offline or send them sexually-provocative images or perform sex acts on webcams they share with people they encounter online. They cyberbully each other by advertising their victims for sexual services, posting real or manufactured sexually explicit images of them online or by passing online rumors able their sexual preferences or activities.

Preteens and Teens at Risk: Most of the high risk preteens and teens fall into three categories: those who are naive and looking for love and affection (typically the "loners"

and "shy" preteens and teens), those who already engage in other high risks activities, such as drug and alcohol abuse, driving too fast or doing risky things for the thrill of it (often the student leaders, athletes, cheerleaders and very competitive teens, the risks takers and thrill seekers looking to let off steam or impress their peers) and those who don't realize that what they do online is real, the ones who are looking to appear older, cooler, more fun and more popular (most of the teens and especially preteens fall into this category at least once). Sadly, most of our preteens and teens fit one of these categories. Sadder still is the fact that in recent years we have learned that most preteens and teens are potential victims.

Naive, loners and socially-shy preteens and teens: Some believe that they are communicating with a cute 14 year old boy, who they later discover isn't cute, isn't fourteen and isn't a boy. Most of the reported cases fall into this category, and until the death of Christina Long four years ago this May, experts all believed that *all* victims fell into this category. They are conned, and easy to spot online. Predators can seek them out, and find their vulnerabilities. They are groomed with care, and often fall in love with their molesters. Sadly, when the molestation finally occurs, not only are their bodies broken, their hearts and trust are too.

They need to understand how the predators work online. Too often they tell me that they can "tell" how old someone is online. They can't. No one can. Many predators spend years cultivating the right tone and language to look like a fellow teen online.

These preteens and teens are sitting ducks. While they may have learned not to fall for the "help me find my puppy" ploy offline, they need to learn how that same ploy (appeal for assistance) works online. They need to know how to spot the risks and the predators, when online everyone can look like a cute 14 year old boy. They need to learn that romance shouldn't occur only in cyberspace, and that parents can get involved to help them meet their soul-mate, assuming they really are. So, if they aren't, and turn out to be a 46 year old child molester, they can come home safely and help put that molester behind bars where they deserve.

Risk-takers, Thrill-seeking preteens and teens: Some preteens and teens (mainly teens) are looking for the thrills and challenge of engaging in a relationship (or at least prolonged communication) with an adult. They "play games" with the adult, and are intentionally extra sexually-provocative. They think they are smart enough to do this without getting hurt. They see this as a game, without realizing the consequences of their actions. And crossing the sexual line isn't as frightening online as it would be in real life. The problem is that the consequences are not as apparent, the realities not as immediate. They take risks. And they think they can handle them. (They don't often understand the consequences, though.) They often willingly engage in sexual communications with men they know are adults. That's part of the thrill. They are also often willing to engage in sexual activities with the adult, but don't realize what that can mean when things go very wrong. We rarely hear about these kinds of victims, because they never report it when things go wrong. They feel as though they "asked for it," or are to blame. When we hear of these cases, it's because they are killed or kidnapped. (Christina Long was in this category. She was the first confirmed murder victim of an Internet sexual predator in the U.S. and died four years ago this May.)

Friends are the answer here. If we can get friends too help watch out for each other, it is less likely that they will meet adults in real life, or if they do, got alone. Also, finding cool

spokespeople, like Nick Lachey, to explain that it isn't cool to be stupid and campaigns such as our "Don't Be Stupid" help. So do real life stories from victims themselves about how they got caught and advice from the trenches. Kateisplace.org has sections specifically directed at this type of victim. And Teen People is an important partner of ours in spreading the word.

Not really a drunken slut, just playing one online: We've all been reading about this new trend in the news (often with me as the expert). Good, respectful, otherwise well-mannered preteens and teens acting out in cyberspace. In profiles, blogs, on social networking sites and their away messages on IM, on their websites and interactive gaming bios, they act out. They pose in their bras, or worse. They simulate sexual activities (and in some cases post images of actual sexual activities). They pretend to be someone or something other than what they really are. And this alter-ego may be a sexually promiscuous teen "up for anything."

They don't think it is cool to tell others they were home coloring with their five year old niece last weekend. Instead they claim to have snuck out after everyone was asleep to get drunk at a wild party. To them it isn't real. They lie. They pose. They do thing online they would never dream of doing in RL. They aren't really drunken sluts - they are just playing one online. (Shannon, one of our award-winning Teenangels, will share insight into why teens and preteens are doing this, during her testimony today.)

The Anatomy of a Cyberpredator:

There have been many cases recently where pedophiles and other adults have lured children into offline meetings and molested them. Luckily, there are even more cases when such attempts to lure a child have brought about the attention of law-enforcement groups. I debated whether I should discuss any of these cases, because I did not want to sensationalize them. But if explaining the methods used by offenders might make parents more aware, and their children safer, it’s worth it.

Cyberpredators, just like their offline counterparts, usually aren’t the scary, hairy monsters in trench coats we imagine standing on a dark street corner. Many are the kind of person you would be inviting to your home as a guest, and often have. They are pediatricians, teachers, lawyers, clergy, vice cops, welfare workers, journalists, Boy Scout leaders, baseball coaches, scientists, etc. They are almost always men. (Sometimes women are accomplices, but rarely are women the molesters.) They are often articulate and well-educated. They come in all shapes, sizes, and colors, and they can be very rich or out of work. But they have one thing in common: they want your child.

Most of us are sickened at the thought of an adult having sexual relations with a child, but to be able to protect our children, we must get into the mind of the predator. First of all, predators often don’t see themselves as predators. They see themselves as loving partners with the children they molest. To them this isn’t rape, it’s a seduction. And, as with any seduction, it’s a slow and painstaking process. (Predators have been known to wait more than two years, collecting data on a particular child, before striking.) That’s what makes them hard to detect. They don’t appear to your child to be dangerous.

An FBI agent who shared a panel with me recently said it best: “Before the Internet, these people had to get physically close to your children. They had to lurk near schoolyards, or playgrounds. Kids would see them. Adults would see them. It was a dangerous situation

to be in for them, because everyone would notice an adult male lurking around children. They often had to take jobs and volunteer positions that allowed them to work with children in a position of trust in order to reach their victims. Now, however, the personal risks the pedophiles had to expose themselves to in order to be around children are gone. Now they can be 'one of the kids' and hang out with your kids online without exposing themselves. As long as they don't say or do something in the public room that makes them stand out, they can stay there forever, taking notes."

And, many of them do. They have been known to create large databases on children. They track the children's likes and dislikes. They track information such as whose parents are divorced, who doesn't like their father's new girlfriend or their mother's boyfriend, or who likes computer games or a particular rock group. Kids often share personal information about their lives in chatrooms or on profiles. This is one reason why they shouldn't. The more the predator knows about your child, the more easily they can "groom" them or appear to be their soulmate.

Some cyberpredators (known as "travelers" to law enforcement) seek out the good kids, the smart ones, the ones who are not street-smart and are from sheltered suburban or rural families. Many of our children match that profile perfectly. Others, however, target (or are targeted by) popular, super achiever, risk preferring teens. It took the death of a young teen from Connecticut, Christina Long, before we realized that many of the incidents involved teens who did not fit the loner profile. What we learned was that these kids never report any attacks or exploitation. The only time we hear of these cases is when the teen is kidnapped or killed.

So who is a typical victim of an Internet sexual predator? Anyone between 11-1/2 and 15. All are vulnerable.

It Doesn't Take Torture for Them to Spill Their Guts

Here's a mock chatroom discussion that my law-enforcement friends and I agree is pretty realistic. Imagine a predatorial pedophile sitting and taking notes on this child, and using this information to lure them later. Would your child fall for this? Most, unfortunately, would. This one is more typical of a boy victim and predator communication than a girl victim communication.

Child: I hate my mom! I know it's her fault that my parents are getting divorced.
Predator: I know. My parents are getting divorced, too.
Child: We never have any money anymore, either. Every time I need something, she says the same thing: "We can't afford it." When my parents were together, I could buy things. Now I can't.
Predator: Me too. I hate that!
Child: I waited for six months for the new computer game to come out. My mom promised to buy it for me when it came out. She promised! Now it's out. Can I buy it? Nope. "We don't have enough money!" I hate my mom!
Predator: Oh! I'm so sorry! I got it! I have this really kewl uncle who buys me things all the time. He's really rich.
Child: You're sooooo lucky. I wish I had a rich and kewl uncle.
Predator: Hey! I got an idea! I'll ask my uncle if he'll buy you one too....I told you he's really kewl. I bet he'd say yes.
Child: Really!? Thanks!!
Predator: BRB [cybertalk for "be right back"]... I'll go and call him.

- - -
Predator: Guess what? He said okay. He's gonna buy you the game!
Child: Wow, really? Thanks. I can't believe it!!!
Predator: Where do you live?
Child: I live in NJ. What about you?
Predator: I live in New York. So does my uncle. New Jersey isn't far.
Child: Great!
Predator: Is there a mall near you? We can meet there.
Child: Okay. I live near the GSP Mall.
Predator: I've heard of that. No prob. What about Saturday?
Child: Kewl.
Predator: We can go to McDonald's too if you want. We'll meet you there at noon.
Child: Okay. Where?
Predator: In front of the computer game store. Oh! My uncle's name is George. He's really kewl.
Child: Great... thanks, I really appreciate it. You're so lucky to have a rich and kewl uncle.

Saturday arrives, and the child goes to the mall and meets an adult outside the computer game store. He identifies himself as "Uncle George" and explains that his nephew is already at the McDonald's waiting for them. The child is uncomfortable, but the uncle walks into the store and buys the $100 game. He comes out and hands it to the child, who is immediately neutralized and delighted. Stranger-danger warnings are not applicable. This isn't a stranger—he's "Uncle George," and if any proof was needed, the computer game is it. He gets into Uncle George's car without hesitation to meet his friend at McDonald's. The rest is reported on the 6 o'clock news.

It's disgusting. It makes us sick to our stomachs, but it happens. Not very often, but often enough that you need to be forewarned. (Several thousand cyberpredator cases are opened each year by law enforcement agents in the United States.) But no matter how often it happens, even once is too often. Knowing how they operate and the tricks of the trade will help us teach our child how to avoid being victimized. Each case differs, but the predators tend to use the same general tactics. Aside from the "bait and switch" scam discussed above, they often attempt to seduce a child. They want the child to "want" them.

The Script—How They Operate Online

They begin by striking up a conversation with the child, trying to create a relationship of trust and friendship. They often masquerade as another child or teenager, typically of the opposite sex, unless the child has indicated homosexual interests. (The child may or may not know the "seducer's" real age by the time they meet face-to-face.) Phone calls usually start at this point. Sometimes gifts are sent to the child as well, which may include a Polaroid camera and film. Once they have broken down barriers of caution, they begin introducing sexual topics gradually, often with the use of child pornography to give the child the impression that other children are regularly involved in sexual activities.

Then they begin to approach the child's own sexuality and curiosity, by asking questions and giving them "assignments," like wearing special underwear, sending sexually suggestive photos of themselves to the pedophile, or performing certain sexual acts. These assignments eventually broaden to the exchange of sexually explicit photographs (using the Polaroid, cell phone camera or digital camera) or videos of the child. Finally, the pedophile attempts to arrange a face-to-face meeting. (He may also have divulged his

true age or an age closer to his actual age at this point.)

Why It Works

All the lectures we have given our children from the time they are very young about not talking to strangers aren't applicable online, where everyone is a stranger. A large part of the fun online is talking to people you've never met. In addition, our children's stranger-danger defenses are not triggered when other kids are involved. The warnings apply only to adult strangers, not to other children.

If any of us walked up to a child in a playground and tried to strike up a conversation, they would ignore us and probably run away. But if an unknown eleven-year-old came up to another eleven-year-old in the same playground, they'd be playing in ten seconds flat! That's how the pedophiles get in under our kids' stranger-danger radar—they pretend to be other kids. And children often believe what they read and hear. They "know" things about the predator because they believe what he told them. They also believe what they read about him in his "staged" profile, which supports what he told them. So it's not just true, it's confirmed.

There are many stages at which the pedophile can be thwarted by an observant parent. In addition, children with healthy friendships and a strong, open, and trusting relationship with their parents are less likely to fall victim to pedophiles online. Pedophiles typically prey on a child's loneliness. They feed the child's complaints about her home life—creating an "us-versus-them" atmosphere. "Your mom is so mean to you! I don't know why she won't let you _____." (Fill in the blank with whatever we try and limit: makeup, malls, concerts, etc.)

This atmosphere does two things: It creates a distance between the child and her parents, at the same time bringing the child into a special secret alliance with the pedophile. (You should know that boys are almost as often the victims of Internet sexual exploitation as girls are, but they report it less frequently.)

I have followed many cases over the last few years. In my role as WiredSafety executive director, I've also been responsible for reporting several of these to law enforcement and for helping many families through the pain of prosecution. Sometimes we just help the families survive what the molestation has done to them. (The child isn't the only victim—entire families are torn apart in the aftermath of a molestation.) Parents feel guilty for not having protected their child, siblings don't know how to treat their fellow sibling—the pain can continue for a lifetime, and even more. And, in addition to being hurt physically, the young victim's heart is broken by the betrayal of trust.

Anatomy of a Real and Early Case

One case I reviewed many years ago involved a New Jersey teenager and an Ohio adult predator. It was one of the earliest reported cases of cyber-predatorial conduct, discovered in 1996. Luckily, the liaison was discovered before the girl met the man face-to-face. But it had gone on for a year and a half before being discovered by the girl's mother. As you read the details, think about what could have been done to discover the situation earlier and how you can use these precautions to protect your children.

Paul Brown, Jr., an Ohio resident, was forty-six years old. He was also unemployed, weighed over four hundred pounds, and lived in a basement. He had accounts with several ISPs. Mary (a hypothetical name for the young girl involved) was twelve when her

mother, a schoolteacher, bought her a computer, reportedly because Mary was having problems making friends. When she got online, Mary posted a message on an online service, in the spring of 1995, looking for a pen pal. In her message she described herself as a teenage girl. Paul Brown, Jr., responded to the message, using his real name (something they often do, surprisingly) but identifying himself as a fifteen-year-old boy.

Brown and Mary maintained an e-mail and telephone relationship for several months. As the relationship became more involved, they began writing letters, and Mary sent Brown a photograph. He told her that he was living at home with his mother and was hoping to find a girlfriend. In early August, Brown asked Mary for a "favor." "If I sent you a roll of film, could you get one of your friends to take pictures of you in different outfits and maybe hairstyles? Makeup if you use any, and different poses. Some sexy, if possible. Please. Baby for me. Thanx. You're the best. Love Ya."

Mary complied. For the next eight months, they continued to converse and correspond, and Mary sent additional photos. Brown encouraged her with juvenile antics, such as using stickers in his letters to her saying things like "Getting better all the time!" In May 1996, Brown sent Mary a special love note. "Saying I love you... seems to be an understatement. At the age of 14 you have captured my heart and made it sing... I love everything about you…."

Shortly thereafter, Brown confessed to being in his twenties. He also suggested that Mary videotape herself in sexually provocative poses. She did. After Brown had reviewed her videotape, he returned it to her with instructions to redo the tape and include views of her genitalia and breasts. He later admitted to being divorced and in his thirties. He reportedly also sent her small gifts from time to time.

A few months later, in response to Brown's promise to pass copies of the tape to four members of a rock band Mary admired, she sent additional videotapes to Brown. (Brown told Mary that he knew the band members very well.) Each tape sent to Brown was designated for a different member of the band and contained sexually explicit conduct. Brown apparently had also sent her his size 48 underwear. When her mother discovered the underwear, the authorities were notified. Tracing Brown through phone records, special agents of the FBI in Cleveland seized the videotapes and photos of Mary and of more than ten other teenage girls from across the country.

Mary was fourteen when this was all discovered. Brown pled guilty to enticing a minor to produce sexually explicit photos and videos and was sentenced to a little less than five years in prison (the maximum penalty for a first offense). In a written statement to Brown following all of this, Mary said, "I trusted you. I thought you were my friend."

There are several things that stand out in this case. One, interstate phone calls were made by Mary. Parents should always be reviewing long-distance bills for suspicious calls. Two, Mary was lonely. These kinds of children are often the most vulnerable; a parent should be involved in their online friendships, and monitor their online lives. And, three, as hard as it is to know what our kids are doing when we're not around, especially if you are a single parent, a year and a half is a long time for a relationship to be going on undiscovered. You should spend time learning who your children's friends are, online and off. But Monday-morning quarterbacking is always easier than playing the game in real time. We may look at the situation and say that could never happen to one of our kids. However, there but for the grace of God go all of us....

Knowing your child is lonely and has problems making friends is the first sign that the child may fall prey to a pedophile or cyber- predator. Predators can spot lonely children. They can also spot kids who are new online and may not yet know all the rules. Most teens, when surveyed, admit to having been propositioned online. But what may be obvious to a cyberstreetsmart kid may not be so obvious to a child not yet familiar with cyberspace. Pedophiles befriend these kids and patiently build trust and a relationship—looking toward the day when they can meet face-to-face.

Encourage your children to make online friends, but learning about their online friends is an important way to avoid these secret relationships. Education is important in avoiding this danger, too. (Had Mary been forewarned about how pedophiles operate online, she may have been more attentive to how old Brown sounded on the phone, and been more aware of his classic tactics.) So is control over incoming and outgoing information when younger children are involved, using technology blockers, monitors, and filters. These kinds of situations can be avoided if you plan ahead, educate and communicate with your children, and keep your eyes open.

Getting in Under Your Radar:

Even when parents are watching, bad things can happen.

I included the Paul Brown case in my first book, A Parents' Guide to the Internet. (He was sentenced in 1997, when I wrote the book.) I included it because it was a good example of how cyberpredators typically operate, and suggested that if the mother had been a bit more attentive, it might have been discovered earlier. I was right about how cyberpredators operate. I was wrong about how being attentive might have avoided the sexual exploitation. It takes more. It takes both an attentive parent and a teenager who has been taught how these pedophiles operate online.

In November 1998, I met a mother who did everything right. She was attentive and inquisitive about her daughter's online relationships. She asked the right questions. She had a good relationship with her daughter, and yet Charles Hatch, a child molester from Utah, got in under everyone's radar and sexually exploited her thirteen-year-old daughter.

Jennifer (not her real name) was eleven and a half when she first met "Charlie" online. She thought he was a few years older, and was intrigued about befriending a slightly older teenage boy. Jennifer was an honors student and had already been taking advanced college courses while still in middle school. She lived in a loving and warm household with her mother and father. She also had siblings and half siblings from her father's previous marriage. They were all close.

Jennifer's mother, Sharry (also not her real name), talked to Jennifer about her online friend, Charlie. She insisted on talking to Charlie himself, by phone, once he and Jennifer had started calling each other. He passed the phone call test, and Sharry was convinced that he really was the teenage boy he professed to be. Either he had manipulated his voice to sound younger or he had a younger person make the call. Charlie even called and spoke to Jennifer's brothers, talking about when he would be their brother-in-law someday, after he and Jennifer were married. He pleaded with Jennifer to come and visit him in Utah. Sharry invited him to visit them instead. But Charlie always had a reason he couldn't come.

As things progressed, Sharry insisted on talking to Charlie's mother. He first avoided it by saying she was sick, later that her sickness had become cancer, and that eventually she died from the cancer. The family fell for this, hook, line, and sinker. Most caring families would. Although the "relationship" progressed for almost two years, it remained relatively tame. Charlie was romantic rather than predatorial, and he sent her expensive gifts, including a Polaroid camera. (Remember the Polaroid camera Paul Brown sent?)

Jennifer was inexperienced with boys and dating, and Charlie seemed to know not to push her too fast. But about a year and a half after they met online, Charlie sent her sexually explicit photos of himself from the neck down. She became very uncomfortable and pulled back. But several tragedies occurred around the same time, which made Jennifer easier prey. Her father was hospitalized with a serious illness, and her sixteen-year-old half brother died of a brain hemorrhage.

Charlie, like all good predators, knew when to strike. He told Jennifer that she owed him sexually explicit photos of herself, since he had sent those of himself. When she refused, he told her that she would be left alone, since her family was dying or would die—and he threatened to leave her. Reluctantly, after fighting against it as hard as she could, she acquiesced and sent him sexually explicit photos of herself.

When Sharry was cleaning Jennifer's room, she discovered a letter in which Charlie had set forth the sexual poses he wanted Jennifer to photograph. Sharry sent him a letter, confronting him. She said that he didn't sound like a teenager in the letter. She told him that if he ever contacted her daughter again, she would inform the police. He never replied, and Jennifer was not permitted to use the Internet for months.

One day, just when Jennifer and Sharry thought that the whole episode was past them, the phone rang. It was a detective from Utah, who informed Sharry that Jennifer's photos had been discovered in Hatch's day planner by a coworker. He wasn't sixteen—he was thirty-six. He was a former teacher who had been dismissed by the school after having been accused by a student of sexual abuse. (The school hadn't taken any other action.) He was currently employed by the welfare office in Utah, and was married with children and step-children.

Six months later, Charles Hatch was convicted of sexual exploitation in a Utah federal court. He began his six-and-a-half year sentence in early June 1999. As a condition of his plea, he will not be permitted to use the Internet. This mother has become a dear friend of mine, after seeking WiredSafety' help in getting through this. She was the first parent to speak out publicly about her child being targeted by a sexual predator online.

Unfortunately, the predators are willing to try many different ploys until one finally works.

Using Celebrity's Names

I was having lunch in Los Angeles with one of my girlfriends when Nick Lachey walked into the restaurant. She pointed him out to me and I immediately grabbed my business card and approached his table (to the utter embarrassment of my friend). I introduced myself and told him I needed his help. I explained that predators were using his name and the name of other celebrities to lure kids into meetings and unsafe activities. They find

teens who post their favorite celebrities on their profiles, websites or other online communications. Then they create a profile claiming to be a close personal friend of that celebrity. They offer to forward a pic of the teen to the celebrity, and seek sexier and sexier pics as time goes on, ultimately ending with an offer to introduce the teen to their favorite celebrity in real life. Years ago, Justin Timberlake was the most popular of these celebrity lures. Nick is now. He listened intently and turned white when he realized people where using his name to hurt his young fans. He offered his help.

When I left his table, he has agreed to do a public service announcement to help teens understand that is anyone claims to be a close personal friend of a celebrity, they aren't. Or won't be for long. I was very excited, but not as excited as I was two weeks later when someone from Nick's office called asking me to help them create a safer teen-only social networking site called YFly.com. I agreed and YFly.com became a reality with the financial assistance of Tom Petters (and the Petters Group), and the creativity and energy of its founders, Drew Levin and Daniel Perkins. I joined the team to set up a safer network and create the most advanced educational and awareness content online, just for teen users. The young users can click on "Report the Creep" if they suspect someone is an adult posing as a teen.

It's a beginning. Finding safer technologies and services is part of the solution. So is awareness using teenspeak.

Shannon, one of our Teenangels is 14 years old. She was selected by Teen People as one of the twenty teens who will make a difference. She has gone them one better...she is already making a difference. It is with pride that I introduce Shannon Sullivan, one of my Teenangels.

[Appendixes omitted]

Appendix 9: Parenting Online

Parenting Online

What do we do when our eight-year-old knows more than we do about cyberspace? How do we guide our children safely through this new world? How do we set the rules when we don't even understand the risks? The childproof locks, seatbelts and helmets we use to help keep them safe in everyday life won't protect them in cyberspace. There we need new and different gadgets and safety tips.

Welcome to the new world of parenting online! It's your newest challenge. But don't worry...it's not as hard as you think and it's well worth the effort.

Parenthood is never easy and the ground rules are always changing. We go from playing the role of confidante, to co-conspirator, to police chief, to teacher, to playmate and back...all in the same day. We barely have the chance to catch our breath!

The things we do to make sure our children stay safe are constantly changing too. When they crawl, we learn how to keep things off the floor. Then, they pull themselves upright, we have to keep them safe from the new dangers at eye level. Training wheels have to be removed, and we have to watch while they pedal away (generally into the nearest tree). We watch their sugar intake, make sure they take their vitamins and keep small items out of their mouths.

That's our job, as parents. So the tried and true warnings, passed down from generation to generation, are repeated... "don't talk to strangers...," "come straight home from school...," "don't provoke fights...," "don't tell anyone personal information about yourself..." and "we need to meet your friends..." This is familiar territory after all. We know the dangers our kids face in the street or at the mall or in the school yard, because we faced them.

As in any large community, there are dangers our children encounter in cyberspace, too. But, since our children know more than we do about cyberspace, we worry about how we can teach them to avoid those dangers. Don't panic... those dangers can be managed using the same old warnings we've always used.

We just need to translate them into cyberspace terms...

And there are wonders around every cyber-corner too...

The Internet is the largest collection of information in the world, always available without a charge and delivered to your home computer. Every question you might have can be answered online. When your child asks you how deep the ocean is or why the sky is blue, you can "ask the Internet," together.

You and your children can communicate with others too, worldwide and in every language, with the click of your mouse. Their artwork can be displayed, their news reporting published and their poems posted on the largest "refrigerator door" in the universe, where 700 million people can appreciate them.

You can research your family tree and build a family Web site. And, best of all...the most complicated homework assignment can be researched online (even last-minute on the Sunday night before it's due).

You can search online for just about anything and any information you want. The easiest way to do that is by using search engines. You can type your search into one of the search engines and often will find what you are seeking. Just as often, though, you will find sites that are trying to get your or your children's attention. Pornographers are the most frequent abusers of search engines, registering and coding their sites to trick people into visiting them, thinking they are Disney, Pokemon or even the White House.

Most of the search engines now have filtering options. By selecting one of these options, most inappropriate content is filtered out and the search results are typically kid-friendly. Two commercial search engines were designed just for kids, though, and are wonderful places to begin your child's search online. Yahooligans!, Yahoo! kid-sized search engine hand-selects the sites, making sure nothing slips through. It is best for younger children, ten and under. Ask Jeeves for Kids is Ask Jeeves kid-sized search engine. Although not as scrubbed clean as Yahooligans! hand-selected sites, it contains many more sites which make it perfect for slightly older children. I recommend it for children ten and older.

In addition, most full-size search engines have a filtered option you can select. But remember that even if you use a search engine filter, if the kids search for images, the can find things you wish they hadn't. That's when using a filtering product that can block images too might come in handy.

In addition to kid-sized search engines, there are many wonderful family-friendly site lists. WiredKids has one of its own, where the sites are selected and reviewed by our specially-trained volunteers. You can even recommend your favorite sites to be added.

There are some entertaining sites that teach children online safety, as well. Although we

prefer our WiredKids.org, StopCyberbullying.org and InternetSuperHeroes.org the best, (she says modestly...) another very special one we want to point out. Disney's Surfswellisland.com teaches online safety Disney-style. Mickey Mouse, Donald Duck, Minnie Mouse and Goofy all find themselves involved in tropical island cyber-challenges relating to viruses, privacy, netiquette (cyber-etiquette) and responsible surfing. Lesson plans, online safety worksheets and other wonderful resources are all available without charge at the site.

Looking for homework help? Check out Discovery.com, Nationalgeographic.org, PBSkids.org and The National Gallery of Art kids page www.nga.gov/kids/kids.htm**.** And ask your school librarian or the librarian at your public library for sites they recommend. Librarians and library media specialists are the guides to valuable and safe online resources for children. And if you need something you can't find, send me an email at “Ask Parry,” (askparry@wiredsafety.org) my Internet-syndicated online safety column. Drop by WiredKids.org or WiredSafety.org to find out how to submit a question.

- **Don't talk to or accept anything from strangers.** That's the first one we learn while growing up, and the first one we teach our children. The problem in cyberspace though is teaching "stranger danger." Online, it's hard to spot the strangers.

The people they chat with enter your home using your computer. Our kids feel safe with us seated nearby. Their "stranger" alerts aren't functioning in this setting. Unless they know them in real life, the person is a stranger no matter how long they have chatted online. Period. You need to remind them that these people are strangers, and that all of the standard stranger rules apply.

You also must teach them that anyone can masquerade as anyone else online. The "12-year-old" girl they have been talking to may prove to be forty-five year old man. It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace.

- **Come straight home after school.** Parents over the generations have always known that children can get into trouble when they wander around after school. Wandering aimlessly online isn't any different. Parents need to know their children are safe, and doing something productive, like homework. Allowing your children to spend unlimited time online, surfing aimlessly, is asking for trouble.

Make sure there's a reason they're online. If they are just surfing randomly, set a time limit. You want them to come home after they're done, to human interaction and family activities (and homework).

- **Don't provoke fights.** Trying to provoke someone in cyberspace is called "flaming." It often violates the "terms of service" of your online service provider and will certainly get a reaction from other people online.

Flaming matches can be heated, long and extended battles, moving from a chat room or discussion group to e-mail quickly. If your child feels that someone is flaming them, they should tell you and the sysop (system operator, pronounced sis-op) or moderator in charge right away and get offline or surf another area. They shouldn't try to defend themselves or get involved in retaliation. It's a battle they can never win.

- **Don’t take candy from strangers.** While we don’t take candy form people online, we do often accept attachments. And just like the offline candy that might be laced with drugs or poisons, a seemingly innocent attachment can destroy your computer files, pose as you and destroy your friends or spy on you without you even knowing it. Use a good anti-virus, update it often and try one of the new spyware blockers. You can get a list of the ones we recommend at WiredSafety.org. Practice safe computing!

- **Don't tell people personal things about yourself.** You never really know who you're talking to online. And even if you think you know who you are talking to, there could be

strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard.

With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at Web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly.

- **We need to get to know your friends.** Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.

- **R-E-S-P-E-C-T.** We all know the golden rule. We have a special one for cyberspace. Don't do anything online you wouldn't do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. You can learn more about the ways to combat cyberbullying at our new website, StopCyberbullying.org or at WiredSafety.org's cyberstalking and harassment section. Remember that it is just as likely that your child is a cyberbully (sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

Remember that the new handheld and interactive gaming devices you buy have real risks to. Your children can send and receive text-messages from anyone on their cell phones or text-messaging devices and interactive games allow them to chat, on Internet phone, to anyone who wants to talk with them. The new Bluetooth devices let your child receive messages form anyone in a 300 foot range, and could be a problem if they play the new Bluetooth handheld games in a mall. Think about the features you are buying when you buy new devices for your children. Check into privacy and security settings. Our Teenangels (teenangels.org) are working on new guides for parents and other teens on what to look for and think about before you buy a new interactive device. Look for them at your local retailer or on the WiredSafety.org and Teenangels.org websites.

Don't just set up the computer in the corner of their bedroom, and leave them to surf alone. Take a look at their computer monitor every once in awhile, it keeps them honest. Sit at their side while they compute when you can. It will help you set rules that make sense for your child. It also gives you an unexpected benefit...you'll get a personal computing lesson from the most affordable computer expert you know!

And it's worth the effort. When our children surf the Internet, they are learning skills that they will need for their future. They become explorers in cyberspace, where they explore ideas and discover new information.

Also, because there is no race, gender or disability online, the Internet is the one place where our children can be judged by the quality of their ideas, rather than their physical attributes.

What Tech Tools Are Out There?
Blocking, filtering and monitoring...when you need a little help

There are many tools available to help parents control and monitor where their children surf online. Some even help regulate how much time a child spends playing computer games, or prevent their accessing the Internet during certain preset times.

I've listed the type of protections that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. Recently, given parents' concerns about strangers communicating with their children online, monitoring software has gained in popularity. Although it might have its place in protecting a troubled child, it feels more like "spyware" than child protection. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. AOL's parental controls were the first of these to be developed and used. MSN 8.0 launched the first set of parental controls for MSN. To read more about the various products and services we have reviewed, visit WiredKids.org and WiredSafety.org.

Blocking Software
Blocking software is software that uses a "bad site" list. It blocks access to sites on that list. They may also have a "good site" list, which prevents your child from accessing any site not on that list. Some of the software companies allow you to customize the lists, by adding or removing sites from the lists. I recommend you only consider software that allows you to customize the list, and lets you know which sites are on the lists.

Filtering
Filtering software uses certain keywords to block sites or sections of sites on-the-fly. Since there is no way any product can keep up with all the sites online, this can help block all the sites which haven't yet been reviewed. The software blocks sites containing these keywords, alone or in context with other keywords.

Some companies allow you to select certain types of sites to block, such as those relating to sex, drugs or hate. This feature engages special lists of keywords that match that category. As with the "bad site" lists, the lists of keywords used by the filtering software should be customizable by the parent, and every parent should be able to see which terms are filtered.

Outgoing Filtering
No... this doesn't mean your software had a sparkling personality :-) (that's cyberspace talk for "grin" and means you're supposed to smile at my brilliant humor, and if you want to learn more about this stuff...you need to read my Ms. Parry's Guide to Correct Online Behavior). It means that your child won't be able to share certain personal information with others online. Information such as your child's name, address or telephone number can be programmed into the software, and every time they try to send it to someone online, it merely shows up as "XXXs." Even with kids who know and follow your rules, this is a terrific feature, since sometimes, even the most well-intentioned kids forget the rules.

Monitoring and Tracking
Some software allows parents to track where their children go online, how much time they spend online, how much time they spend on the computer (such as when they are playing games) and even allows parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside of the home,

or with working single-parents, who want to make sure their children aren't spending all of their time on the computer. Many parents who don't like the thought of filtering or blocking, especially with older children and teens, find monitoring and tracking satisfy their safety concerns. They can know, for sure, whether their children are following their rules.

We particularly recommend using a monitoring software and then forgetting it’s installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations, where your child went to meet an adult offline. We particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is key to keeping your children safe online.

Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or child safety caps. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology protection available, unless your children know what to expect and how to react when they run into something undesirable online, they are at risk. Arming them well means teaching them well.

Your Online Safety “Cheatsheet”
Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn't spend all of her time on the computer. People, not computers, should be their best friends and companions.

- Keep the computer in a family room, kitchen or living room, not in your child's bedroom. Remember that this tip isn’t very helpful when your children have handheld and mobile Internet and text-messaging devices. You can’t make them keep their cell phones in a central location. So make sure that the “filter between their ears” is working at all times.

- Learn enough about computers so you can enjoy them together with your kids.

- Teach them never to meet an online friend offline unless you are with them.

- Watch your children when they're online and see where they go.

- Make sure that your children feel comfortable coming to you with questions and don't over react if things go wrong.

- Keep kids out of chat rooms or IRC unless they are monitored.

- Encourage discussions between you and your child about what they enjoy online.

- Discuss these rules, get your children to agree to adhere to them, and post them near the computer as a reminder.

- Find out what e-mail and instant messaging accounts they have and (while agreeing not to spy on them) ask them for their passwords for those accounts.

- “Google” your children (and yourself) often and set alerts for your child’s contact information. The alerts will e-mail you when any of the searched terms are spotted online. It’s an early warning system for cyberbullying posts, and can help you spot ways in which your child’s personal information may be exposed to strangers online. To learn how to “Google” them, visit InternetSuperHeroes.org.

- Teach them what information they can share with others online and what they can't (like telephone numbers, address, their full name, cell numbers and school).

- Check your children’s profiles, blogs and any social-networking posts. Social-networking websites include myspace.com, facebook.com and xanga.com. (We work closely with MySpace and Facebook to help keep their users safer.) Social networks, generally, shouldn’t be used by preteens and should be only carefully used by teens. Yfly.com is a new teen-only social network that is designed from top to bottom to keep teens safer and teach them about more responsible behaviors.

- For those of you with preteens and young teens, read the Safer Social Networking guide at WiredSafety.org.

- Get to know their "online friends" just as you get to know all of their other friends.

- Warn them that people may not be what they seem to be and that people they chat with are not their friends, they are just people they chat with.

- If they insist on meeting their online friend in real life, consider going with them. When they think they have found their soul mate, it is unlikely that your telling them “no” will make a difference. Offering to go with them keeps them safe.

- Look into the new safer cell phones and cell phone features that give you greater control over what your children can access from their phone and how can contact them.

PARENTING ONLINE

MY AGREEMENT ABOUT USING THE INTERNET

Once you understand enough about cyberspace and how your children surf the Internet, you can set your own rules. These are the basic rules, even though you may want to add some of your own.

Some kids like setting the rules out clearly in an agreement. Here's one you can use, and post near your computer to help them remember how to surf safely. (Note that while the tips may work for teens, the contract is designed for preteens and younger.)

I want to use our computer and the Internet. I know that there are certain rules about what I should do online. I agree to follow these rules and my parents agree to help me follow these rules:

1. I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number, to anyone I meet online.

2. I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really grown ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any e-mails I get from or send e-mails to new people I meet online.

3. I will not buy or order anything online without asking my parents or give out any credit card information.

4. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.

5. I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.

6. If I see something I do not like or that I know my parents don't want me to see, I will click on the "back" button or log off.

7. If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.

8. I won't keep online secrets from my parents.

9. If someone sends me any pictures or any e-mails using bad language, I will tell my parents.

10. If someone asks me to do something I am not supposed to do, I will tell my parents.

11. I will not call anyone I met online, in person, unless my parents say it's okay.

12. I will never meet in person anyone I met online, unless my parents say it's okay.

13. I will never send anything to anyone I met online, unless my parents say it's okay.

14. If anyone I met online sends me anything, I will tell my parents.

15. I will not use something I found online and pretend it's mine.

16. I won't say bad things about people online, and I will practice good netiquette.

17. I won't use bad language online.

18. I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.

19. I will help teach my parents more about computers and the Internet.

20. I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.

21. I won't post my cell number on my away message, and will check with someone before posting something personal about me on my blog or on a networking site.

22. I will Stop, Block and Tell! If I am harassed online or cyberbullied.

23. I will Take 5! before reacting to something that upsets me or makes me angry online.

24. I will practice responsible "thinkB4Uclick" rules. (I know I can find out more about these things at InterentSuperHeroes.org and StopCyberbullying.org.)

25. I will learn how to be a good cybercitizen and control the technology, instead of being controlled by it.

_____

I promise to follow these rules. (signed by the child)

_____

I promise to help my child follow these rules and not to over react if my child tells me about bad things in cyberspace (signed by parent).

From Parry:

I am asked questions about kids online safety at least a hundred times a day. Is the Internet a dangerous place? Are there predators out there looking to set up a meeting with my child? How can we find good and reliable content online? How can I supervise my child's surfing when I can't even turn on the computer?

These any other question like these fill my inbox daily. (If you have a question of your own, visit WiredKids.org or WiredSafety.org and click on "Ask Parry." Here is the one simple answer:

The single greatest risk our children face in connection with the Internet is being denied access. We have solutions for every other risk.

That bears repeating, over and over, especially when we hear about Internet sexual predators, hate, sex and violence online. But our children need the Internet for their education, careers and their future.

Happily, most of the risks are easily confined. In each and every case when children encounter Internet sexual predators offline, they go willing to the meeting. They may think the person is a cute fourteen year old girl or boy, but they know they are meeting someone they don't know in real life. That means we can prevent 100% of these crimes. Merely teach our children not to meet Internet strangers offline. If they are set on meeting that person anyway, go with them. That way, if the person turns out to be a cute fourteen year old, you are the hero. And if they aren't, you're an even *bigger* hero.

Our WiredKids, WiredTeens and Teenangels programs, in addition to being fun and educational sites, are also volunteer programs where children and teens are taught online safety and privacy and responsible surfing. They then use these skills to help other children and teens learn to surf safely, as well. Talk to your children about what they do online (and offline also), and let them know you are there to help if things go wrong. You will note that in our safe surfing agreement parents have to promise only one thing...not to overreact if their children come to them for help. Earn their trust, and be worthy of it. Register your children at WiredKids.org, our children's online safety site, and we will make sure they learn what they need to know about enjoying the Internet safely and privately. It's not about technology at all...it's about communication and good parenting.

Remember, we're all in this together!

Parry
Parry Aftab, Esq.
Executive Director
WiredSafety.org and its family of sites and programs, including Teenangels.org, WiredKids.org and CyberLawEnforcement.org